CN 1266328A which corresponds to USP6,693,965

[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
H04N 1/387
G09C 5/00 G06T 9/00

[12]发明专利申请公开说明书

[21]申请号 00101628.8

[43]公开日 2000年9月13日

[11]公开号 CN 1266328A

[22]申请日 2000.1.21 [21]申请号 00101628.8

[30]优先权

[32]1999.1.22 [33]JP [31]015011/1999

[32]1999.5.19 [33]JP [31]138914/1999

[71]申请人 松下电器产业株式会社

地址 日本国大阪府

[72]发明人 井上尚 桂卓史

[74]专利代理机构 上海专利商标事务所

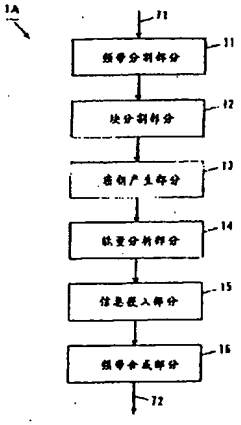
代理人 李 玲

权利要求书 11 页 说明书 38 页 附图页数 23 页

[54]发明名称 嵌入和提取数字信息的装置和方法、以及载有程序的媒体

[57]摘要

一种嵌入和提取数字信息的装置和方法，频带分割部分11将图象信号71分割成10个频带，计算子波系数。块分割部分12将MRA分量分割成多个预定的块。密钥产生部分13从具有预定值的密钥找出一个二级密钥，产生表示该二级密钥是否用于嵌入的信息。能量分析部分14计算子波系数的能量。若不小于预定设定值，信息嵌入部分15把数字信息嵌入到MRA分量的块的子波系数中。频带合成部分16将嵌入处理后的MRA分量与MRR分量相合成，重构图象信号72。



ISSN1008-4274

权 利 要 求 书

1. 一种将固有数字信息嵌入在数字图象信号中的数字信息嵌入装置，其特征在于所述装置包括：

利用离散子波变换或是子带分割将所述数字图象信号分割成多个频带以获得子波系数的频带分割装置(11)；

以预定的块尺寸将通过分割获得的所述频带当中待嵌入所述数字信息的频带(以下称为嵌入目标区域)分割成多个块的块分割装置(12)；

对于组成所述数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的密钥产生装置(13)；

基于每个所述产生的二级密钥指定所述嵌入目标区域中的块，并将组成所述数字信息的相应信息分别嵌入到所述嵌入目标区域的指定块的子波系数中的信息嵌入装置(15)；以及

利用嵌入处理后的所述嵌入目标区域和所述嵌入目标区域以外的多个频带重构其中嵌入了所述数字信息的数字图象的频带合成装置(16)。

2. 一种将固有数字信息嵌入在数字图象信号中的数字信息嵌入装置，其特征在于所述装置包括：

利用离散子波变换或是子带分割将所述数字图象信号分割成多个频带以获得子波系数的频带分割装置(11)；

以预定的块尺寸将通过分割获得的所述频带当中待嵌入所述数字信息的频带(以下称为嵌入目标区域)分割成多个块的块分割装置(12)；

对于组成所述数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的密钥产生装置(13)；

基于每个所述所产生二级密钥指定所述嵌入目标区域中的块，以及分别计算多个频带中除所述嵌入目标区域以外的每一个频带的对应于与所述嵌入目标区域中指定块位置相同的空间表示区域的子波系数的能量的能量分析装置(14)；

控制所述密钥产生装置(13)以致于当所述能量小于预定的设定值时产生另一个二级密钥，以及当所述能量不小于预定的设定值时将组成所述数字信息的相应信息分别嵌入到所述嵌入目标区域的指定块的子波系数中的信息嵌入

装置(15)；以及

利用嵌入处理后的所述嵌入目标区域和所述嵌入目标区域以外的多个频带重构其中嵌入了所述数字信息的数字图象的频带合成装置(16)。

3. 如权利要求 2 所述的数字信息嵌入装置，其特征在于进一步包括：

当能量在不小于所述预定设定值和不大于预定上限值的范围时使已经计算出其能量的子波系数乘以一预定值 U(U 是不小于 1 的实数)，而当能量在小于所述预定设定值但不小于预定下限值的范围时使子波系数乘以一预定值 L(L 是不大于 1 的实数)的系数相乘装置(31)。

4. 一种在特定频带(以下称为嵌入目标区域)的子波系数中提取由特定装置所嵌入的固有数字信息的数字信息提取装置，所述特定频带是利用离散子波变换或是子带分割通过对数字图象信号进行分割所获得的，其特征在于所述装置包括：

接收由所述特定装置输出的重构数字图象信号，利用离散子波变换或是子带分割将所述数字图象信号分割成多个频带以获得子波系数的频带分割装置(11)；

以预定的块尺寸将通过分割获得的所述频带当中的所述嵌入目标区域分割成多个块的块分割装置(12)；

对于组成所述数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的密钥产生装置(13)；

基于每个所述产生的二级密钥指定所述嵌入目标区域中的块，以及从所述嵌入目标区域的所述指定块的子波系数中分别检测组成所述被嵌入数字信息的信息的信息检测装置(21)。

5. 一种在特定频带(以下称为嵌入目标区域)的子波系数中提取由特定装置所嵌入的固有数字信息的数字信息提取装置，所述特定频带是利用离散子波变换或是子带分割通过对数字图象信号进行分割所获得的，其特征在于所述装置包括：

接收由所述特定装置输出的重构数字图象信号，利用离散子波变换或是子带分割将所述数字图象信号分割成多个频带以获得子波系数的频带分割装置(11)；

以预定的块尺寸将通过分割获得的所述频带当中的所述嵌入目标区域分

割成多个块的块分割装置(12)；

对于组成所述数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的密钥产生装置(13)；

基于每个所述所产生二级密钥指定所述嵌入目标区域中的块以及分别计算多个频带中除所述嵌入目标区域以外的每一个频带的对应于与所述嵌入目标区域中指定块位置相同的空间表示区域的子波系数的能量的能量分析装置(14)；以及

从能量不小于预定设定值的所述嵌入目标区域的块的子波系数中分别检测组成被嵌入数字信息的信息的信息检测装置(21)。

6.一种将固有数字信息嵌入到数字图象信号中的数字信息嵌入装置，其特征在于所述装置包括：

将所述数字图象信号分割成多个块的块分割装置(41)，每个块由多个预定象素组成；

对通过分割所获得的每个所述块进行频率变换，以计算频率系数的频率变换装置(42)；

从所述计算出的频率系数当中选择一个特定频率系数串以及寻找该频率系数串的绝对平均值 M 和能量的系数计算装置(43)；

对于能量不小于预定阈值的所述频率系数串，利用预定的量化步长 Q(Q 是不小于 1 的整数)让所述找到的绝对平均值 M 经受线性量化以计算量化值的量化装置(44)；

基于所述量化值和所述数字信息的值用预定值替换量化值的信号替换装置(45)；

利用所述量化步长 Q 使所述已替换量化值经受逆线性量化以计算平均值 M'以及利用平均值 M'与所述绝对平均值 M 之间的差 DM(=M'-M)校正所述频率系数的系数校正装置(46)；以及

让所述校正后的多个块经受逆频率变换，以重构已经嵌入了所述数字信息的数字图象的逆频率变换装置(47)。

7.如权利要求 6 所述的数字信息嵌入装置，其特征在于：

所述系数计算装置(43)选择低频分量中除 DC 分量以外的频率系数串。

8.如权利要求 6 所述的数字信息嵌入装置，其特征在于：

当所述量化值等于所述阈值除以所述量化步长 Q 的值时，所述系数校正装置(46)将预定的设定值加到所述差值 DM 上。

9. 如权利要求 6 所述的数字信息嵌入装置，其特征在于：

当所述差值 DM 是负数以及所述频率系数的绝对值小于该差值 DM 的绝对值时，所述系数校正装置(46)将频率系数校正为 0。

10. 一种从通过将数字图象信号分割成块并使每个块经受频率变换而获得的特定频率系数中提取由特定装置所嵌入的固有数字信息的数字信息提取装置，其特征在于所述装置包括：

接收由所述特定装置输出的数字图象信号，按照由所述特定装置进行的所述块分割将所述数字图象信号分割成多个块的块分割装置(41)，每个块由多个预定象素组成；

按照由所述特定装置进行的所述频率变换对通过分割所获得的每个所述块进行频率变换，以计算频率系数的频率变换装置(42)；

按照由所述特定装置进行的计算方法从所述计算出的频率系数当中选择一个特定频率系数串，寻找频率系数串的绝对平均值 M 和能量的系数计算装置(43)；

对于能量不小于预定阈值的所述频率系数串，利用所述特定装置所采用的量化步长 Q 使所述绝对平均值 M 经受线性量化以计算量化值的量化装置(44)；以及

判定所述量化值是偶数还是奇数，并基于判定结果提取被嵌入的所述数字信息的信息提取装置(51)。

11. 一种将固有数字信息嵌入在数字图象信号中的方法，其特征在于所述方法包括：

利用离散子波变换或是子带分割将所述数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割获得的所述频带当中待嵌入所述数字信息的频带(以下称为嵌入目标区域)分割成多个块的步骤(S201)；

对于组成所述数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤(S206)；

基于每个所述产生的二级密钥指定所述嵌入目标区域中的块并将组成所

述数字信息的相应信息分别嵌入到所述嵌入目标区域的指定块的子波系数中的步骤(S210、S215)；以及

利用嵌入处理后的所述嵌入目标区域和所述嵌入目标区域以外的多个频带重构其中嵌入了所述数字信息的数字图象的步骤。

12. 一种将固有数字信息嵌入在数字图象信号中的方法，其特征在于所述方法包括：

利用离散子波变换或是子带分割将所述数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割获得的所述频带当中待嵌入所述数字信息的频带(以下称为嵌入目标区域)分割成多个块的步骤(S201)；

对于组成所述数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤(S206)；

基于每个所述所产生二级密钥指定所述嵌入目标区域中的块，并分别计算多个频带中除所述嵌入目标区域以外的每一个频带的对应于与所述嵌入目标区域中指定块位置相同的空间表示区域的子波系数的能量的步骤(S210-S212)；

控制所述密钥产生步骤(13)以致于当所述能量小于预定的设定值时产生另一个二级密钥的步骤(S213)；

当所述能量不小于预定的设定值时将组成所述数字信息的相应信息分别嵌入到所述嵌入目标区域的指定块的子波系数中的步骤(S215)；以及

利用嵌入处理后的所述嵌入目标区域和所述嵌入目标区域以外的多个频带重构其中嵌入了所述数字信息的数字图象的步骤。

13. 如权利要求 12 所述的方法，其特征在于进一步包括：

当能量在不小于所述预定设定值和不大于预定上限值的范围时使已经计算了其能量的子波系数乘以一预定值 U(U 是不小于 1 的实数)，而当能量在小于所述预定设定值但不小于预定下限值的范围时使子波系数乘以一预定值 L(L 是不大于 1 的实数)的步骤(S1401 至 S1404)。

14. 一种从特定频带(以下称为嵌入目标区域)的子波系数中提取由特定装置所嵌入的固有数字信息的方法，所述特定频带是利用离散子波变换或是子带分割通过对数字图象信号进行分割所获得的，其特征在于所述方法包括：

接收由所述特定装置输出的重构数字图象信号，利用离散子波变换或是子带分割将所述数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割获得的所述频带当中的所述嵌入目标区域分割成多个块的步骤(S1201)；

对于组成所述数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤(S1206)；以及

基于每个所述产生的二级密钥指定所述嵌入目标区域中的块，并从所述嵌入目标区域的指定块的子波系数中分别检测组成所述被嵌入数字信息的信息的步骤(S1201 和 S1214)。

15. 一种在特定频带(以下称为嵌入目标区域)的子波系数中提取由特定装置所嵌入的固有数字信息的方法，所述特定频带是利用离散子波变换或是子带分割通过对数字图象信号进行分割所获得的，其特征在于所述方法包括：

接收由所述特定装置输出的重构数字图象信号，利用离散子波变换或是子带分割将所述数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割获得的所述频带当中的所述嵌入目标区域分割成多个块的步骤(S1201)；

对于组成所述数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤(S1206)；

基于每个所述所产生二级密钥指定所述嵌入目标区域中的块，并分别计算多个频带中除所述嵌入目标区域以外的每一个频带的对应于与所述嵌入目标区域中指定块位置相同的空间表示区域的子波系数的能量的步骤(S1210 至 S1212)；以及

从能量不小于预定设定值的所述嵌入目标区域的块的子波系数中分别检测组成被嵌入数字信息的信息的步骤(S1214)。

16. 一种将固有数字信息嵌入到数字图象信号中的方法，其特征在于所述方法包括：

将所述数字图象信号分割成多个块的步骤，每个块由多个预定象素组成；

对通过分割所获得的每个所述块进行频率变换，以计算频率系数的步骤；

从所述计算出的频率系数当中选择一个特定频率系数串以及寻找该频率系数串的绝对平均值 M 和能量的步骤(S1702 和 S1703)；

对于能量不小于预定阈值的所述频率系数串，利用预定的量化步长 Q(Q 是不小于 1 的整数)使所述找到的绝对平均值 M 经受线性量化以计算量化值的步骤(S1705)；

基于所述量化值和所述数字信息的值用预定值替换量化值的步骤(S1707 至 S1712)；

利用所述量化步长 Q 使所述已替换量化值经受反线性量化以计算平均值 M'，并利用平均值 M'与所述绝对平均值 M 之间的差 DM(=M'-M)校正所述频率系数的步骤(S1703 至 S1717)；以及

让所述校正后的多个块经受逆频率变换，以重构已经嵌入了所述数字信息的数字图象的步骤。

17. 如权利要求 16 所述的嵌入数字信息的方法，其特征在于：

在所述寻找步骤(S1702 至 S1703)中，选择低频分量中除 DC 分量以外的频率系数串。

18. 如权利要求 16 所述的嵌入数字信息的方法，其特征在于：

在所述校正步骤(S1713 至 S1717)中，当所述量化值等于所述阈值除以所述量化步长 Q 的值时，将预定的设定值加到所述差值 DM 的值上。

19. 如权利要求 16 所述的嵌入数字信息的方法，其特征在于：

在所述校正步骤(S1713 至 S1717)中，当所述差值 DM 是负数以及所述频率系数的绝对值小于差 DM 的绝对值时，将频率系数校正为 0。

20. 一种从通过将数字图象信号分割成块并使每个块经受频率变换而获得的特定频率系数中提取由特定装置所嵌入的固有数字信息的方法，其特征在于所述方法包括：

接收由所述特定装置输出的数字图象信号，按照由所述特定装置进行的所述块分割将所述数字图象信号分割成多个块的步骤，每个块由多个预定象素组成；

按照由所述特定装置进行的所述频率变换对通过分割所获得的每个所述块进行频率变换，以计算频率系数的步骤；

按照由所述特定装置进行的计算方法从所述计算出的频率系数当中选择所述特定频率系数串，以及寻找该频率系数串的绝对平均值 M 和能量的步骤(S2002 至 S2003)；

对于能量不小于预定阈值的所述频率系数串，利用所述特定装置所采用的量化步长 Q 使所述绝对平均值 M 经受线性量化以计算量化值的步骤(S2005)；以及

判定所述量化值是偶数还是奇数，以及基于判定结果提取嵌入的所述数字信息的步骤(S2006 至 S2008)。

21. 一种记录媒体，在计算机中可执行的程序记录在其上，所述程序是指在所述计算机上实现的一种操作环境，其特征在于包括：

利用离散子波变换或是子带分割将所述数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割获得的所述频带当中待嵌入所述数字信息的频带(以下称为嵌入目标区域)分割成多个块的步骤(S201)；

对于组成所述数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤(S206)；

基于每个所述产生的二级密钥指定所述嵌入目标区域中的块并将组成所述数字信息的相应信息分别嵌入到所述嵌入目标区域的指定块的子波系数中的步骤(S210、S215)；以及

利用嵌入处理后的所述嵌入目标区域和所述嵌入目标区域以外的多个频带重构其中嵌入了所述数字信息的数字图象的步骤。

22. 一种记录媒体，在计算机中可执行的程序记录在其上，所述程序是指在所述计算机上实现的一种操作环境，其特征在于包括：

利用离散子波变换或是子带分割将所述数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割获得的所述频带当中待嵌入所述数字信息的频带(以下称为嵌入目标区域)分割成多个块的步骤(S201)；

对于组成所述数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤(S206)；

基于每个所述所产生二级密钥指定所述嵌入目标区域中的块以及分别计算多个频带中除所述嵌入目标区域以外的每一个频带的对应于与所述嵌入目标区域中指定块位置相同的空间表示区域的子波系数的能量的步骤(S210-S212)；

控制所述密钥产生步骤以致于当所述能量小于预定的设定值时产生另一个二级密钥的步骤(S213)；

当所述能量不小于预定的设定值时将组成所述数字信息的相应信息分别嵌入到所述嵌入目标区域的该指定块的子波系数中的步骤(S215)；以及

利用嵌入处理后的所述嵌入目标区域和所述嵌入目标区域以外的多个频带重构其中嵌入了所述数字信息的数字图象的步骤。

23. 如权利要求 22 所述的记录媒体，其特征在于进一步包括：

当能量在不小于所述预定设定值和不大于预定上限值的范围时使已经计算了其能量的子波系数乘以一预定值 U(U 是不小于 1 的实数)，而当能量在小于所述预定设定值但不小于预定下限值的范围时使子波系数乘以一预定值 L(L 是不大于 1 的实数)的步骤(S1401 至 S1404)。

24. 一种记录媒体，在计算机中可执行的程序记录在其上，所述程序是指在所述计算机上实现的一种操作环境，其特征在于包括：

对于由特定装置嵌入在利用离散子波变换或子带分割通过对数字图象信号进行分割所获得的特定频带(以下称为嵌入目标区域)内的子波系数中的固有数字信息，接收由所述特定装置输出的重构数字图象信号，并利用离散子波变换或是子带分割将所述数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割获得的所述频带当中的所述嵌入目标区域分割成多个块的步骤(S1201)；

对于组成所述数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤(S1206)；以及

基于每个所述产生的二级密钥指定所述嵌入目标区域中的块，并从所述嵌入目标区域的指定块的子波系数中分别检测组成所述被嵌入数字信息的信息的步骤(S1201 和 S1214)。

25. 一种记录媒体，在计算机中可执行的程序记录在其上，所述程序是指在所述计算机上实现的一种操作环境，其特征在于包括：

对于由特定装置嵌入在利用离散子波变换或子带分割通过对数字图象信号进行分割所获得的特定频带(以下称为嵌入目标区域)内的子波系数中的固有数字信息，接收由所述特定装置输出的重构数字图象信号，并利用离散子波

变换或是子带分割将所述数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割获得的所述频带当中的所述嵌入目标区域分割成多个块的步骤(S1201)；

对于组成所述数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤(S1206)；

基于每个所述所产生二级密钥指定所述嵌入目标区域中的块以及分别计算多个频带中除所述嵌入目标区域以外的每一个频带的对应于与所述嵌入目标区域中指定块位置相同的空间表示区域的子波系数的能量的步骤(S1210 至 S1212)；以及

从能量不小于预定设定值的所述嵌入目标区域的块的子波系数中分别检测组成被嵌入数字信息的信息的步骤(S1214)。

26. 一种记录媒体，在计算机中可执行的程序记录在其上，所述程序是指在所述计算机上实现的一种操作环境，其特征在于包括：

将所述数字图象信号分割成多个块的步骤，每个块由多个预定象素组成；

对通过分割所获得的每个所述块进行频率变换，以计算频率系数的步骤；

从所述计算出的频率系数当中选择一个特定频率系数串，并寻找该频率系数串的绝对平均值 M 和能量的步骤(S1702 和 S1703)；

对于能量不小于预定阈值的所述频率系数串，利用预定的量化步长 Q(Q 是不小于 1 的整数)使所述找到的绝对平均值 M 经受线性量化以计算量化值的步骤(S1705)；

基于所述量化值和所述数字信息的值用预定值替换量化值的步骤(S1707 至 S1712)；

利用所述量化步长 Q 使所述已替换量化值经受逆线性量化以计算平均值 M' 以及利用平均值 M' 与所述绝对平均值 M 之间的差 DM(=M'-M)校正所述频率系数的步骤(S1703 至 S1717)；以及

让所述校正后的多个块经受逆频率变换，以重构已经嵌入了所述数字信息的数字图象的步骤。

27. 如权利要求 26 所述的记录媒体，其特征在于：

在所述寻找步骤(S1702 至 S1703)中，选择低频分量中除 DC 分量以外的频

率系数串。

28. 如权利要求 26 所述的记录媒体，其特征在于：

在所述校正步骤(S1713 至 S1717)中，当所述量化值等于所述阈值除以所述量化步长 Q 的值时，将预定的设定值加到所述差值 DM 的值上。

29. 如权利要求 26 所述的记录媒体，其特征在于：

在所述校正步骤(S1713 至 S1717)中，当所述差值 DM 是负数以及所述频率系数的绝对值小于差 DM 的绝对值时，将频率系数校正为 0。

30. 一种记录媒体，在计算机中可执行的程序记录在其上，所述程序是指在所述计算机上实现的一种操作环境，其特征在于包括：

对于由特定装置嵌入在通过将数字图象信号分割成块以及让每个块经受频率变换所获得的特定频率系数串中的固有数字信息，接收由所述特定装置输出的数字图象信号，按照由所述特定装置进行的块分割将所述数字图象信号分割成多个块的步骤，每个块由多个预定象素组成；

按照由所述特定装置进行的所述频率变换对通过分割所获得的每个所述块进行频率变换，以计算频率系数的步骤；

按照由所述特定装置进行的计算方法从所述计算出的频率系数当中选择一个特定频率系数串以及寻找频率系数串的绝对平均值 M 和能量的步骤(S2002 至 S2003)；

对于能量不小于预定阈值的所述频率系数串，利用所述特定装置所采用的量化步长 Q 使所述绝对平均值 M 经受线性量化以计算量化值的步骤(S2005)；以及

判定所述量化值是偶数还是奇数，并基于判定结果提取所嵌入的所述数字信息的步骤(S2006 至 S2008)。

说　明　书

嵌入和提取数字信息的装置和方法、以及载有程序的媒体

本发明涉及嵌入和提取数字信息的装置和方法以及其上记录有执行该方法的程序的媒体，尤其涉及为了保护数字数据的版权将诸如版权信息(下文中称为数字信息)的数字数据嵌入图象信号中和提取所嵌入数字信息的装置和方法以及其上记录有进行该方法的程序的媒体。

近年来，已经能够利用因特网广泛地提供信息，尤其是，已经能够频繁地利用 WWW(环球网)提供图象、语音等综合信息的信息发送/接收服务。

然而，公布在因特网的网络上的诸如图象的数字数据很容易被许多非指定用户所复制。因此，便出现了一些问题。例如，未得到版权拥有人的许可，通过越权复制二次利用第三人拥有其版权的图象。此外，在利用基于图象的内容在因特网上扩大商务中，防止越权复制的措施也已经成为一个问题。因此，需要建立保护图象信号的版权的技术。

电子(数字)水印技术便是通常所知措施的一个例子。数字水印是一种以不能被人们所感觉到的形式将数字信息嵌入在图象数据中的技术。

传统数字水印技术的例子有：利用 Matsui、Ohnishi、Nakamura 在题目为“在子波变换下将签字嵌入图象”(电子、信息和通信工程协会杂志 D-II Vol. J79-D-II No. 6, pp. 1017-1024, 1996 年 6 月)(在下文中称为 Matui 等人的技术)的文章中所描述的离散子波变换的数字水印技术。此外，另一个例子是利用 Nakamura、Ogawa、Takashima 在题目为“为保护数字图象版权的在频域下的水印方法”(加密术和信息安全性专集，SCIS'97-26A，1997 年 1 月)(下文中称为 Nakamura 等人的技术)的文章中所描述的利用离散余弦变换(DCT)的数字水印技术。

首先参考图 23 至 25 描述 Matui 等人的技术。

首先将描述通过离散子波变换处理的带分割。图 23 是表明分割成三个分层的传统频带分割装置 11 的结构例子的方框图。在图 23 中，传统的频带分割装置 11 包括第一至第三带分割滤波器 100、200 和 300，它们具有相同结构。第一至第三带分割滤波器 100、200 和 300 中每一个将输入图象分割成四个频

带，并计算每个频带的子波系数。对于子波系数，将进行次级带分割，这里不作描述。

频带分割装置 11 将数字化图象信号 71 输入到第一带分割滤波器 100。第一带分割滤波器 100 基于其水平和垂直分量的参数将图象信号 71 分割成四个带的信号，即 LL1 信号、LH1 信号、HL1 信号和 HH1 信号(以下统称为第一分层信号)。第二带分割滤波器 200 接收第一分层信号中最低带内的 LL1 信号，将 LL1 信号进一步分割成四个带中的 LL2 信号、LH2 信号、HL2 信号和 HH2 信号(以下统称为第二分层信号)。第三带分割滤波器 300 接收第二分层信号中最低带内的 LL2 信号，将 LL2 信号进一步分割成四个带中的 LL3 信号、LH3 信号、HL3 信号和 HH3 信号(以下统称为第三分层信号)。

图 24 是表明图 23 所示的第一带分割滤波器 100 的详细结构例子的方框图。在图 24 中，第一带分割滤波器 100 包括第一至第三双频带分割部分 101 至 103。第一至第三双频带分割部分 101 至 103 分别包括一维低通滤波器(LPF)111 至 113、一维高通滤波器(HPF)121 至 123、和以 2:1 的比例对信号进行抽取的子取样器 131 至 133 和 141 至 143。

第一双频带分割部分 101 接收图象信号 71，由 LPF 111 和 HPF 121 使图象信号 71 针对其水平分量分别经过低通滤波和高通滤波输出两个信号。利用子取样器 131 和 141 以 2:1 的比例分别对通过低通滤波和高通滤波所获得的信号进行抽取，然后输出到后续阶段。第二双频带分割部分 102 接收来自子取样器 131 的信号，由 LPF 112 和 HPF 122 针对其垂直分量对信号分别进行滤波，获得两个信号，利用子取样器 132 和 142 以 2:1 的比例对信号进行抽取，然后输出信号，即 LL 信号和 LH 信号。另一方面，第三双频带分割部分 103 接收来自子取样器 141 的信号，由 LPF 113 和 HPF 123 针对其垂直分量对信号分别进行滤波，获得两个信号，利用子取样器 133 和 143 以 2:1 的比例对信号进行抽取，然后输出信号，即 HL 信号和 HH 信号。

因此，四个信号，即在其水平和垂直分量上都低的 LL1 信号、在其水平分量上低而在其垂直分量上高的 LH1 信号、在其水平分量上高而在其垂直分量上低的 HL1 信号、在其水平和垂直分量上都高的 HH1 信号，即子波系数从第一带分割滤波器 100 输出。第二和第三带分割滤波器 200 和 300 使接收的信号也分别经过与如上所述相同的处理。

作为由第一至第三带分割滤波器 100、200 和 300 进行的带分割处理的结果，图象信号 71 被分割成 10 个带信号，即 LL3 信号、LH3 信号、HL3 信号、HH3 信号、LH2 信号、HL2 信号、HH2 信号、LH1 信号、HL1 信号和 HH1 信号。图 25 是表明由两维频域表示 10 个带信号的示意图。

在图 25 中，垂直轴代表垂直频率分量，它向下表示增大，水平轴代表水平频率分量，它向右表示增大。图 25 所示的每个区域是用作一个图象的数据，区域的面积比例与带信号中各个数据数目的比例相一致。即，在 LL3 信号、LH3 信号、HL3 信号和 HH3 信号(它们是第三分层信号)中数据数目取为 1 的情况中，LH2 信号、HL2 信号和 HH2 信号(它们是第二分层信号)中的数据数目取为 4，LH1 信号、HL1 信号和 HH1 信号(它们是第一分层信号)中的数据数目取为 16。因此，例如，针对 LL3 信号的左上方的一个数据，LH3 信号、HL3 信号和 HH3 信号中每一个的左上方处的一个数据，LH2 信号、HL2 信号和 HH2 信号中每一个的左上方处的 4 个正方形数据，LH1 信号、HL1 信号和 HH1 信号中每一个的左上方处的 16 个正方形数据代表原始图象上的相同象素(图 25 中的阴影部分)。

现在描述在为带分割进行上述离散子波变换后嵌入数字信息的方法。接下来描述的嵌入方法是本领域专业人员公知的技术。Matui 等人通过将离散子波变换与传统嵌入方法相结合实现了数字水印。

传统的嵌入方法利用人们易于忽视高频域中的噪声而检测低频域中噪声的视觉特性。即，在图象信号中，能量集中在其低频分量中。因此，在离散子波变换的输出分量中，代表图象信号低频分量的 LL 信号是一个重要带分量。另一方面，三种类型的多分辨率表示(MRR)分量(它们是代表图象信号高频分量的 LH 信号、HL 信号和 HH 信号)不认为是很重要的带分量。

对于非重要 MRR 分量的 LH 信号、HL 信号和 HH 信号中的每一个，按照基于预定规则被嵌入的数字信息的位值，在 MRR 分量的子波系数当中，对子波系数的低阶位(如果可能，是最低有效位(LSB))的非零逻辑值进行变换，进行数字水印化。

在 Matui 等人的技术中，数字信息仅仅嵌入在 MRR 分量(它们是通过离散子波变换计算的图象的高频分量)及其各自低阶位(它们难以影响图象变化)中。因此，由嵌入了数字信息的信号所重构的图象质量的降低是很轻微的，以致于人眼感觉不到。

在网络上显示和分布的情况中，由频带合成装置对已经经受嵌入处理的各个频带中的信号进行合成(简单地说，进行与离散子波变换相反的处理)，重构图象信号。此外，为了从重构图象信号中提取已嵌入的数字信息，进行离散子波变换，以提取在嵌入处理中所变换的逻辑值。

然而，在上述的 Matui 等人的技术中，数字信息嵌入在 LH1 信号、HL1 信号和 HH1 信号中，它们是最高的高频(MRR)分量，存在下列问题：

1.通过对已经嵌入数字信息的图象的频率变换，然后改写和切割图象的高频分量，能够相对比较简单地去除已嵌入的数字信息。

2.即使通过让已经嵌入数字信息的图象经受低通滤波，也能够降低图象的高频分量，从而丢掉已嵌入的信息。

3.另外，例如在图象通信中，图象是在被压缩时传送的。在这种情况中，通常对频率系数的高频分量进行粗略量化，进行不可逆压缩，从而增大对图象高频分量的影响。即，图象 MRR 分量中的子波系数的各个低阶位被大大改变，所以不能正确地提取已嵌入的信息。

因此，本申请的发明人和其他人在以前提交的“日本专利公开公报 10-196361”(以下称为较早申请)中提出了一种新的数字水印技术，以解决传统数字水印技术中的问题。

较早申请中的嵌入方法是一种当子波系数经过线性量化时按照被嵌入数字信息的位值在其最近附近在对奇数值或偶数值的量化中设定输出值的方法。即，以预定的块尺寸将图象信号的最低频带分量(以下称为 MRA 分量(多分辨率近似分量))分割成多个块，利用上述嵌入方法把数字信息嵌入到每个块的子波系数的平均值中。

在较早申请中，利用量化误差使 MRA(它是通过离散子波变换计算出的图象信号的低频分量)经过数字信息嵌入处理。

接着将简要地描述 Nakamura 等人的技术。

在 Nakamura 等人的技术中，数字图象信号首先被分割成块，在嵌入的情况中每个块由 8×8 个象素组成，使每个块经受 DCT 运算，对其频率进行变换(即，寻找频率系数)。然后从低频分量的频率系数中随机地提取一个频率系数 C，DC 分量(DC 系数)中的一个频率系数除外，按照以下方程式(1)所表示的，利用量化步长 h 再次对频率系数 C 进行量化，寻找量化值 q。函数 int[X]表示

X 的线性量化：

$$q = \text{int}\,[C/h] \times h \qquad (1)$$

在 Nakamura 等人的技术中，如果待嵌入在块中的数字信息的位 b 是“0”基于以下方程式(2)，如果位 b 是“1”基于以下方程式(3)，选择最接近频率系数 C 的整数，以校正频率系数 C 的值。字符 t 表示选择最靠近附近的自然数。

$$C \leftarrow q + ht + q/4 \qquad (2)$$

$$C \leftarrow q + ht + 3q/4 \qquad (3)$$

另一方面，在 Nakamura 等人的技术中，在提取的情况下，首先提取已经嵌入数字信息的频率系数 C，然后利用量化步长 h 由以上方程式(1)进行重新量化，寻找量化值 q。然后找到量化值 q 与频率系数 C 之间的差 p(=C-q)，利用以下方程式(4)或(5)作出判定，提取被嵌入数字信息的位 b 的值：

$$0 \leqq p < h/2 \rightarrow b=0 \qquad (4)$$

$$h/2 \leqq p < h \rightarrow b=1 \qquad (5)$$

因此，在 Nakamura 等人的技术中，通过隐藏利用伪随机数字串嵌入低频分量的频率系数当中 DC 系数以外的频率系数 C 的位置，以及通过引入由利用参数 h 再量化引起的误差分量，第三人几乎没有关于被嵌入数字信息的线索。

然而，在较早的申请中，数字信息嵌入在所有的 MRA 分量(它们是最低频率分量)中，以致于仍然存在下列问题。

1. 正如已经描述的，人的视觉特性通常具有易于忽视高频域中噪声而检测低频域中噪声的性质。此外，图象信号的平坦部分具有的能量几乎集中在 MRA 分量(低频分量)中，图象信号的详细部分对应于 MRR 分量(高频分量)。即，在离散子波变换的输出分量中，如果对应于图象信号平坦部分的 MRA 分量通过嵌入操作而被修正的话，那么，不管修改是如何轻微，图象质量被降低。

2. 以预定块尺寸将 MRA 分量分割成多个块，将数字信息嵌入在所有的块中。因此，一旦公众知道嵌入算法，便可以对被嵌入数字信息进行解码。

另一方面，在 Nakamura 等人的技术中，将数字信息嵌入在所有的块中，所以，在对应于数字图象信号平坦部分的块中，图象质量降低。此外，数字信息仅仅嵌入在低频分量的一个频率系数 C 中。于是，对于第三人所作的越权使用的尝试(例如，图案压缩)，已嵌入的数字信息可能会丢失。

因此，本发明的一个目的是提供一种对应于图象信号详细部分的 MRA 分量

或在较低频带(较深分层信号)的 MRR 分量中嵌入和提取数字信息的装置和方法，使得在解码时几乎不使图象质量劣化，而且几乎不给第三者提供关于被嵌入数字信息的线索。

本发明的另一个目的是提供一种嵌入和提取数字信息的装置和方法，其中数字信息是利用低频分量的频率系数当中 DC 分量以外的多个频率系数的平均值嵌入的，数字信息嵌入在对应于图象信号详细部分的块中，以致于在解码时几乎不使图象质量降低，已嵌入的数字信息也保持着不会丢失(通常，把这称为“数字信息具有抵抗力”)，防止第三者的越权使用的尝试。

本发明的再一个目的是提供一种具有适合 MPEG(活动图象专家组)/JPEG(联合照相专家组)(这是当前图象编码)的数字水印系统。

本发明具有实现上述目的的以下特征。

本发明的第一方面是指一种将固有数字信息嵌入在数字图象信号中的数字信息嵌入装置，包括：

利用离散子波变换或是子带分割将数字图象信号分割成多个频带以获得子波系数的频带分割装置；

以预定的块尺寸将通过分割获得的频带当中待嵌入数字信息的频带(以下称为嵌入目标区域)分割成多个块的块分割部分；

对于组成数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的密钥产生部分；

基于每个产生的二级密钥指定所述嵌入目标区域中的块并将组成数字信息的相应信息分别嵌入到嵌入目标区域的指定块的子波系数中的信息嵌入部分；以及

利用嵌入处理后的嵌入目标区域和嵌入目标区域以外的多个频带重构其中嵌入了数字信息的数字图象的频带合成部分。

如上所述，在第一方面中，数字信息被嵌入在基于二级密钥所指定的块中。因此，不知道产生二级密钥方法的第三人几乎没有被嵌入数字信息的线索。

第二方面是指一种将固有数字信息嵌入在数字图象信号中的数字信息嵌入装置，包括：

利用离散子波变换或是子带分割将数字图象信号分割成多个频带以获得

子波系数的频带分割部分；

以预定的块尺寸将通过分割获得的所述频带当中待嵌入数字信息的频带(以下称为嵌入目标区域)分割成多个块的块分割部分；

对于组成数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的密钥产生部分；

基于每个所产生的二级密钥指定嵌入目标区域中的块以及分别计算多个频带中除嵌入目标区域以外的每一个频带的对应于与嵌入目标区域中指定块位置相同的空间表示区域的子波系数的能量的能量分析部分；

控制密钥产生部分以致于当能量小于预定的设定值时产生另一个二级密钥以及当能量不小于预定的设定值时将组成数字信息的相应信息分别嵌入到嵌入目标区域的指定块的子波系数中的信息嵌入部分；以及

利用嵌入处理后的嵌入目标区域和嵌入目标区域以外的多个频带重构其中嵌入了数字信息的数字图象的频带合成部分。

如上所述，在第二方面中，数字信息是通过判定多个频带的每个频带中除嵌入目标区域以外的对应于基于二级密钥所指定块的位置的子波系数的能量而嵌入的。因此，图象质量在解码时几乎不会降低，第三人几乎没有被嵌入数字信息的线索。

根据第三方面，在第二方面中，装置进一步包括：

当能量在不小于预定的设定值和不大于预定的上限值的范围时使已经计算出其能量的子波系数乘以一预定值 U(U 是不小于 1 的实数)，而当能量在小于预定的设定值但不小于预定的下限值的范围时使子波系数乘以一预定值 L(L 是不大于 1 的实数)的系数相乘部分。

如上所述，在第三方面中，只有在能量接近于预定的设定值时，子波系数才乘以第二方面中的预定值。于是，在能量不小于设定值的情况中，能够防止有误差检测/不完全检测。以防止第三人越权使用(例如，图象压缩)的尝试，因此，能够准确地提取所嵌入的数字信息。此外，图象质量几乎不降低，第三人几乎没有被嵌入数字信息的线索。

第四方面是指一种提取由特定装置嵌入在特定频带(以下称为嵌入目标区域)的子波系数中的固有数字信息的数字信息提取装置，所述特定频带是利用离散子波变换或是子带分割通过对数字图象信号进行分割所获得的，该装置包

括：

接收由特定装置输出的重构数字图象信号，利用离散子波变换或是子带分割将数字图象信号分割成多个频带以获得子波系数的频带分割部分；

以预定的块尺寸将通过分割所获得的频带当中的嵌入目标区域分割成多个块的块分割部分；

对于组成数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的密钥产生部分；

基于每个所产生的二级密钥指定嵌入目标区域中的块以及从嵌入目标区域的指定块的子波系数中分别检测组成被嵌入数字信息的信息的信息检测部分。

如上所述，在第四方面中，被嵌入的数字信息是从基于二级密钥所指定的块中的子波系数检测的。因此，不知道产生二级密钥方法的第三人几乎没有被嵌入数字信息的线索。

第五方面是指一种提取由特定装置嵌入在特定频带(以下称为嵌入目标区域)的子波系数中的固有数字信息的数字信息提取装置，所述特定频带是利用离散子波变换或是子带分割通过对数字图象信号进行分割所获得的，该装置包括：

接收由特定装置输出的重构数字图象信号，利用离散子波变换或是子带分割将数字图象信号分割成多个频带以获得子波系数的频带分割部分；

以预定的块尺寸将通过分割所获得的频带当中的嵌入目标区域分割成多个块的块分割部分；

对于组成数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的密钥产生部分；

基于每个所产生的二级密钥指定嵌入目标区域中的块以及分别计算多个频带中除嵌入目标区域以外的每一个频带的对应于与嵌入目标区域中指定块位置相同的空间表示区域的子波系数的能量的能量分析部分；以及

从能量不小于预定设定值的嵌入目标区域的块的子波系数中分别检测组成被嵌入数字信息的信息的信息检测部分。

如上所述，在第五方面中，判定多个频带中除嵌入目标区域以外的每一个频带的对应于基于二级密钥所指定块位置的子波系数能量，以检测被嵌入数字

信息。因此，不知道产生二级密钥方法的第三人几乎不掌握被嵌入数字信息的线索。

第六方面指一种将固有数字信息嵌入到数字图象信号中的数字信息嵌入装置，该装置包括：

将所述数字图象信号分割成多个块的块分割部分，每个块由多个预定象素组成；

对通过分割所获得的每个块进行频率变换，以计算频率系数的频率变换部分；

从计算出的频率系数当中选择一个特定频率系数串以及寻找该频率系数串的绝对平均值 M 和能量的系数计算部分；

对于能量不小于预定阈值的频率系数串，利用预定的量化步长 Q(Q 是不小于 1 的整数)使找到的绝对平均值 M 经过线性量化以计算量化值的量化部分；

基于量化值和数字信息的值用预定值替换量化值的信号替换部分；

利用量化步长 Q 让已替换量化值经受逆线性量化以计算平均值 M' 以及利用平均值 M' 与绝对平均值 M 之间的差 DM(=M'-M)校正频率系数的系数校正部分；以及

让校正后的多个块经过逆频率变换，以重构已经嵌入了数字信息的数字图象的逆频率变换部分。

如上所述，在第六方面中，判定频率系数串的能量，以嵌入数字信息。因此，在解码时使图象质量几乎不降低，能够保护被嵌入的数字信息不丢失以防止第三人的越权使用的尝试。

根据第七方面，在第六方面中，

所述系数计算部分选择低频分量中除 DC 分量以外的频率系数串。

如上所述，在第七方面中，数字信息被嵌入在第六方面的 DC 分量附近的低频分量的频率系数串中。于是，能够更准确地提取数字信息，不会受越权用户的尝试的影响。

根据第八方面，在第六方面中，

当量化值等于阈值除以量化步长 Q 的值时，系数校正部分将预定的设定值加到差值 DM 上。

如上所述，在第八方面中，在第六方面中对差值 DM 进行运算，以致于在

解码时使图象质量几乎不降低。此外，在能量不小于阈值的情况下，能够阻止有误差检测/不完全检测以防止第三人的越权使用的尝试。因此，能够更准确地提取所嵌入的数字信息。

根据第九方面，在第六方面中，

当差值 DM 是负数以及频率系数的绝对值小于差 DM 的绝对值时，系数校正部分将频率系数校正为 0。

如上所述，在第九方面中，当频率系数的绝对值小于第六方面中差 DM 的绝对值时，不能作出使频率系数的绝对值变得更小的校正，所以使频率系数降低为 0。因此，在数字信息是利用多个频率系数的绝对平均值 M 嵌入的情况中，能够减小误差。于是，能够更准确地提取数字信息。

第十方面是一种提取由特定装置嵌入在特定频率系数串中的固有数字信息的数字信息提取装置，所述特定频率系数串是通过将数字图象信号分割成块并使每个块经过频率变换而获得的，该装置包括：

接收由特定装置输出的数字图象信号，按照由特定装置进行的块分割将数字图象信号分割成多个块的块分割部分，每个块由多个预定象素组成；

按照由特定装置进行的频率变换对通过分割所获得的每个块进行频率变换，以计算频率系数的频率变换部分；

按照由特定装置进行的计算方法从计算出的频率系数当中选择一个特定频率系数串以及寻找该频率系数串的绝对平均值 M 和能量的系数计算部分；

对于能量不小于预定阈值的频率系数串，利用特定装置所采用的量化步长 Q 使绝对平均值 M 经过线性量化以计算量化值的量化部分；以及

判定量化值是偶数还是奇数以及基于判定结果提取所嵌入的数字信息的信息提取部分。

如上所述，在第十方面中，作为提取特定频率系数串的绝对平均值 M 以及利用预定方法计算该频率系数串的绝对平均值的量化值的结果，判定其嵌入数字信息的逻辑值。因此，能够提取准确的数字信息，不受越权用户的尝试的影响。

第十一方面是一种将固有数字信息嵌入在数字图象信号中的方法，包括：

利用离散子波变换或是子带分割将数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割所获得的频带当中待嵌入数字信息的频带(嵌入目标区域)分割成多个块的步骤;

对于组成数字信息的信息,利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤;

基于每个所产生的二级密钥指定嵌入目标区域中的块并将组成数字信息的相应信息分别嵌入到嵌入目标区域的指定块的子波系数中的步骤;以及

利用嵌入处理后的嵌入目标区域和嵌入目标区域以外的多个频带,重构其中嵌入了数字信息的数字图象的步骤。

如上所述,在第十一方面中,数字信息被嵌入在基于二级密钥所指定的块中。因此,不知道产生二级密钥方法的第三人几乎不掌握被嵌入数字信息的线索。

第十二方面是一种将固有数字信息嵌入到数字图象信号中的方法,包括:

利用离散子波变换或是子带分割将数字图象信号分割成多个频带以获得子波系数的步骤;

以预定的块尺寸将通过分割所获得的频带当中待嵌入数字信息的频带(嵌入目标区域)分割成多个块的步骤;

对于组成数字信息的信息,利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤;

基于每个所产生的二级密钥指定嵌入目标区域中的块以及分别计算多个频带中除嵌入目标区域以外的每一个频带的对应于与嵌入目标区域中指定块位置相同的空间表示区域的子波系数的能量的步骤;

当能量小于预定的设定值时控制如产生另一个二级密钥的密钥产生步骤;

当能量不小于预定的设定值时将组成数字信息的相应信息分别嵌入到嵌入目标区域的指定块的子波系数中的步骤;以及

利用嵌入处理后的嵌入目标区域和嵌入目标区域以外的多个频带,重构其中嵌入了数字信息的数字图象信号的步骤。

如上所述,在第十二方面中,判定多个频带中除嵌入目标区域以外的每个频带的对应于基于二级密钥所指定块位置的子波系数的能量,以嵌入数字信息。因此,在解码时几乎不使图象质量降低,而且第三人几乎不掌握所嵌入数

字信息的线索。

根据第十三方面，在第十二方面中，该方法进一步包括：

当能量在不小于预定设定值和不大于预定上限值的范围时使已经计算了其能量的子波系数乘以一预定值 U(U 是不小于 1 的实数)，而当能量在小于预定设定值但不小于预定下限值的范围时使子波系数乘以一预定值 L(L 是不大于 1 的实数)的步骤。

如上所述，在第十三方面，只有当能量接近于第十二方面中的预定设定值时，子波系数才乘以一预定值，由此，在能量不小于设定值的情况下，能够防止有误差检测/不完全检测。以防止第三人的越权使用尝试(例如，图象压缩)，因此，能够准确地提取所嵌入数字信息。此外，使图象质量几乎不降低，对于嵌入数字信息，第三人几乎不掌握线索。

第十四方面是一种提取由特定装置在特定频带(嵌入目标区域)的子波系数中嵌入固有数字信息的方法，特定频带是利用离散子波变换或是子带分割通过对数字图象信号进行分割所获得的，所述方法包括：

接收由特定装置输出的重构数字图象信号，利用离散子波变换或是子带分割将数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割所获得的频带当中的嵌入目标区域分割成多个块的步骤；

对于组成数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤；以及

基于每个所产生的二级密钥指定嵌入目标区域中的块以及从嵌入目标区域的指定块的子波系数中分别检测组成被嵌入数字信息的信息的步骤。

如上所述，在第十四方面中，嵌入数字信息是从基于二级密钥所指定的块的子波系数检测的。因此，不知道产生二级密钥方法的第三人几乎不了解嵌入数字信息的线索。

第十五方面是一种提取由特定装置嵌入在特定频带(嵌入目标区域)的子波系数中的固有数字信息的方法，所述特定频带是利用离散子波变换或是子带分割通过对数字图象信号进行分割所获得的，所述方法包括：

接收由特定装置输出的重构数字图象信号，利用离散子波变换或是子带分割将数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割所获得的频带当中的嵌入目标区域分割成多个块的步骤；

对于组成数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤；

基于每个所产生的二级密钥指定嵌入目标区域中的块以及分别计算多个频带中除嵌入目标区域以外的每一个频带的对应于与嵌入目标区域中指定块位置相同的空间表示区域的子波系数的能量的步骤；以及

从能量不小于预定设定值的嵌入目标区域的块的子波系数中分别检测组成被嵌入数字信息的信息的步骤。

如上所述，在第十五方面中，判定多个频带中除嵌入目标区域以外的对应于基于二级密钥所指定块位置的子波系数的能量，以检测嵌入数字信息。因此，不知道产生二级密钥方法的第三人几乎没有嵌入数字信息的线索。

第十六方面是一种将固有数字信息嵌入到数字图象信号中的方法，包括：

将数字图象信号分割成多个块的步骤，每个块由多个预定象素组成；

对通过分割所获得的每个块进行频率变换，以计算频率系数的步骤；

从计算出的频率系数当中选择一个特定频率系数串以及寻找该频率系数串的绝对平均值 M 和能量的步骤；

对于能量不小于预定阈值的频率系数串，利用预定的量化步长 Q(Q 是不小于 1 的整数)使找到的绝对平均值 M 经过线性量化以计算量化值的步骤；

基于量化值和数字信息的值用预定值替换量化值的步骤；

利用量化步长 Q 使已替换量化值经过逆线性量化以计算平均值 M'，以及利用平均值 M' 与绝对平均值 M 之间的差 DM(=M'-M)校正频率系数的步骤；以及

让校正后的多个块经受逆频率变换，以重构已经嵌入了数字信息的数字图象信号的步骤。

如上所述，在第十六方面中，判定频率系数串的能量，以嵌入数字信息。因此，在解码时使图象质量几乎不降低，而且能够避免嵌入数字信息被丢失，防止第三者的越权使用尝试。

根据第十七方面，在第十六方面中，

在寻找步骤中，选择低频分量中除 DC 分量以外的频率系数串。

如上所述，在第十七方面中，数字信息嵌入在第十六方面的 DC 分量附近

的低频分量的频率系数串中，于是，能够更准确地提取数字信息，不会受越权用户尝试的影响。

根据第十八方面，在第十六方面中，

在校正步骤中，当量化值等于阈值除以量化步长 Q 的值时，将预定的设定值加到差值 DM 上。

如上所述，在第十八方面中，在第十六方面中对差值 DM 进行运算，所以在解码时使图象质量几乎不降低。此外，在能量不小于阈值的情况中能够防止有误差检测/不完全检测防止第三人的越权使用尝试。因此，能够更准确地提取嵌入数字信息。

根据第十九方面，在第十六方面中，

在校正步骤中，当差值 DM 是负数以及频率系数的绝对值小于差 DM 的绝对值时，将频率系数校正为 0。

如上所述，在第十九方面中，当频率系数的绝对值小于第十六方面中差 DM 的绝对值时，不能作出使频率系数的绝对值变得更小的校正，所以使频率系数降低为 0。因此，在利用多个频率系数的绝对平均值 M 嵌入数字信息的情况中，能够降低误差。于是，能够更准确地提取数字信息。

第二十方面是一种提取由特定装置嵌入在特定频率系数串中的固有数字信息的方法，特定频率系数串是通过将数字图象信号分割成块并使每个块经过频率变换而获得的，该方法包括：

接收由特定装置输出的数字图象信号，按照由特定装置进行的块分割将数字图象信号分割成多个块的步骤，每个块由多个预定象素组成；

按照由特定装置进行的频率变换对通过分割所获得的每个块进行频率变换，以计算频率系数的步骤；

按照由特定装置进行的计算方法从计算出的频率系数当中选择一个特定频率系数串以及寻找该频率系数串的绝对平均值 M 和能量的步骤；

对于能量不小于预定阈值的频率系数串，利用特定装置所采用的量化步长 Q 使绝对平均值 M 经受线性量化以计算量化值的步骤；以及

判定量化值是偶数还是奇数以及基于判定结果提取所嵌入的数字信息的步骤。

如上所述，在第二十方面中，作为提取特定频率系数串的绝对平均值 M 以

及利用预定方法计算该频率系数串的绝对平均值 M 的量化值，判定嵌入数字信息的逻辑值。因此，能够准确地提取数字信息，不会受越权用户的尝试的影响。

第二十一方面是一种记录媒体，记录在其上的程序可在计算机中执行，所述程序是指在计算机上实现的一种操作环境，包括：

利用离散子波变换或是子带分割将数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割所获得的频带当中待嵌入数字信息的频带(嵌入目标区域)分割成多个块的步骤；

对于组成数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤；

基于每个所产生的二级密钥指定嵌入目标区域中的块并将组成数字信息的相应信息分别嵌入到嵌入目标区域的指定块的子波系数中的步骤；以及

利用嵌入处理后的嵌入目标区域和嵌入目标区域以外的多个频带，重构其中嵌入了数字信息的数字图象信号的步骤。

第二十二方面是一种记录媒体，记录在其上的程序可在计算机中执行，所述程序是指在计算机上实现的一种操作环境，包括：

利用离散子波变换或是子带分割将数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割所获得的频带当中待嵌入数字信息的频带(嵌入目标区域)分割成多个块的步骤；

对于组成数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤；

基于每个所产生的二级密钥指定嵌入目标区域中的块以及分别计算多个频带中除嵌入目标区域以外的每一个频带的对应于与嵌入目标区域中指定块位置相同的空间表示区域的子波系数的能量的步骤；

当能量小于预定的设定值时控制如产生另一个二级密钥的密钥产生步骤；

当能量不小于预定的设定值时将组成数字信息的相应信息分别嵌入到嵌入目标区域的指定块的子波系数中的步骤；以及

利用嵌入处理后的嵌入目标区域和嵌入目标区域以外的多个频带，重构其中嵌入了数字信息的数字图象的密钥产生步骤。

根据第二十三方面，在第二十二方面中，记录媒体进一步包括：

当能量在不小于预定设定值和不大于预定上限值的范围时，使已经计算了其能量的子波系数乘以一预定值 U，而当能量在小于预定设定值但不小于预定下限值的范围时使子波系数乘以一预定值 L 的步骤。

第二十四方面是一种记录媒体，记录在其上的程序可在计算机中执行，所述程序是指在计算机上实现的一种操作环境，包括：

对于由特定装置嵌入在利用离散子波变换或子带分割通过对数字图象信号进行分割所获得的特定频带(嵌入目标区域)内的子波系数中的固有数字信息，接收由特定装置输出的重构数字图象信号，利用离散子波变换或是子带分割将数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割所获得的频带当中的嵌入目标区域分割成多个块的步骤；

对于组成数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤；以及

基于每个所产生的二级密钥指定嵌入目标区域中的块以及从嵌入目标区域的指定块的子波系数中分别检测组成被嵌入数字信息的信息的步骤。

第二十五方面是一种记录媒体，记录在其上的程序可在计算机中执行，所述程序是指在计算机上实现的一种操作环境，包括：

对于由特定装置嵌入在利用离散子波变换或子带分割通过对数字图象信号进行分割所获得的特定频带(嵌入目标区域)内的子波系数中的固有数字信息，接收由特定装置输出的重构数字图象信号，利用离散子波变换或是子带分割将数字图象信号分割成多个频带以获得子波系数的步骤；

以预定的块尺寸将通过分割获得的频带当中的嵌入目标区域分割成多个块的步骤；

对于组成数字信息的信息，利用预定函数从具有预定值的密钥分别产生具有不同值的二级密钥的步骤；

基于每个所产生的二级密钥指定嵌入目标区域中的块以及分别计算多个频带中除嵌入目标区域以外的每一个频带的对应于与嵌入目标区域中指定块位置相同的空间表示区域的子波系数的能量的步骤；以及

从其能量不小于预定设定值的嵌入目标区域的块的子波系数中分别检测

组成被嵌入数字信息的信息的步骤。

第二十六方面是一种记录媒体，记录在其上的程序可在计算机中执行，所述程序是指在计算机上实现的一种操作环境，包括：

将数字图象信号分割成多个块的步骤，每个块由多个预定象素组成；

对通过分割所获得的每个块进行频率变换，以计算频率系数的步骤；

从计算出的频率系数当中选择一个特定频率系数串以及寻找该频率系数串的绝对平均值 M 和能量的步骤；

对于能量不小于预定阈值的所述频率系数串，利用预定的量化步长 Q 使找到的绝对平均值 M 经过线性量化以计算量化值的步骤；

基于量化值和数字信息的值用预定值替换量化值的步骤；

利用所述量化步长 Q 使已替换量化值经过逆线性量化以计算平均值 M'，并利用平均值 M' 与绝对平均值 M 之间的差 DM(=M'-M)校正频率系数串的步骤；以及

让校正后的多个块经受逆频率变换，以重构已经嵌入了数字信息的数字图象信号的步骤。

根据第二十七方面，在第二十六方面中，

在寻找步骤中，选择低频分量中除 DC 分量以外的频率系数串。

根据第二十八方面，在第二十六方面中，

在校正步骤中，当量化值等于阈值除以量化步长 Q 的值时，将预定的设定值加到差值 DM 上。

根据第二十九方面，在第二十六方面中，

在校正步骤中，当差值 DM 是负数以及频率系数的绝对值小于差 DM 的绝对值时，将频率系数校正为 0。

第三十方面是一种记录媒体，记录在其上的程序可在计算机中执行，所述程序是指在计算机上实现的一种操作环境，包括：

对于由特定装置嵌入在特定频率系数串中的固有数字信息，（特定频率系数串是通过将数字图象信号分割成块以及让每个块经过频率变换所获得的），接收由特定装置输出的数字图象信号，并按照由特定装置进行的块分割将数字图象信号分割成多个块的步骤，每个块由多个预定象素组成；

按照由特定装置进行的频率变换对通过分割所获得的每个块进行频率变

换，以计算频率系数的步骤；

按照由特定装置进行的计算方法从计算出的频率系数当中选择一个特定频率系数串以及寻找该频率系数串的绝对平均值 M 和能量的步骤；

对于能量不小于预定阈值的频率系数串，利用特定装置所采用的量化步长 Q 使绝对平均值 M 经过线性量化以计算量化值的步骤；以及

判定量化值是偶数还是奇数以及基于判定结果提取所嵌入的数字信息的步骤。

如上所述，第二十一至第三十方面是指记录媒体，记录在其上的程序可执行第十一至第二十方面中嵌入和提取数字信息的方法。这对应于以软件形式把第十一至第二十方面的嵌入和提取数字信息的方法提供给现有装置。

从以下的结合附图给出的对本发明的详细描述中，本发明的这些和其它的目的、特征、方面和优点将变得更加清楚。

图 1 是一方框图，表明根据本发明第一实施例的数字信息嵌入装置 1A 的结构。

图 2 是一流程图，表明由图 1 所示的块分割部分 12、密钥产生部分 13、能量分析部分 14 和信息嵌入部分 15 进行的处理。

图 3 是一示意图，表明通过分割 LL3 信号而获得的块的例子。

图 4 是一示意图，表明存储是否采用二级密钥的密钥信息的表的例子。

图 5 是一示意图，表明 LL3 信号中的一个块与对应于同该块位置相同的空间表示区域上的各 MRR 分量之间的位置关系。

图 6 是一方框图，表明图 1 所示的频带合成部分 16 的详细结构例子。

图 7 是一方框图，表明图 6 所示的频带合成滤波器 400 的详细结构例子。

图 8 至 10 是示意图，分别表明将 MRR 分量取作嵌入目标区域的情况中嵌入目标区域与包含用于能量计算的子波系数的频率区域之间的位置关系例子。

图 11 是一方框图，表明根据本发明第二实施例的数字信息提取装置 1B 的结构。

图 12 是一流程图，表明由图 11 所示的块分割部分 12、密钥产生部分 13、能量分析部分 14 和信息检测部分 21 进行的处理。

图 13 是一方框图，表明根据本发明第三实施例的数字信息嵌入装置 2A 的

结构。

图 14 是一流程图，表明由图 13 所示的块分割部分 12、密钥产生部分 13、能量分析部分 14 和系数乘法部分 31 进行的处理。

图 15 是一方框图，表明根据本发明第四实施例的数字信息嵌入装置 3A 的结构。

图 16 是一方框图，表明由图 15 中所示块分割部分 41 和频率变换部分 42 进行的处理例子。

图 17 是一流程图，表明由图 15 所示的系数计算部分 43、量化部分 44、信号替换部分 45 和系数校正部分 46 进行的处理。

图 18 是一示意图，表明由图 15 所示的信号替换部分 45 进行的处理例子。

图 19 是一方框图，表明根据本发明第五实施例的数字信息提取装置 3B 的结构。

图 20 是一流程图，表明由图 19 所示的系数计算部分 43、量化部分 44 和信息提取部分 51 进行的处理。

图 21 是一方框图，表明根据本发明第六实施例的数字信息嵌入装置 4A 的结构。

图 22 是一流程图，表明由图 21 所示的系数计算部分 43、系数乘法部分 61、量化部分 44、信号替换部分 45 和系数校正部分 46 进行的处理。

图 23 是一方框图，表明传统带域分割装置 11 的结构的例子。

图 24 是一方框图，表明图 23 所示的带域分割滤波器的详细结构的例子。

图 25 是一示意图，表明借助于两维频域已经经过由图 23 所示带分割装置 11 的离散子波变换的信号的表示。

(第一实施例)

图 1 是表明根据本发明第一实施例的数字信息嵌入装置结构的方框图。在图 1 中，根据第一实施例数字信息嵌入装置 1A 包括频带分割部分 11、块分割部分 12、密钥产生部分 13、能量分析部分 14、信息嵌入部分 15 和频带合成部分 16。根据第一实施例的数字信息嵌入装置 1A 中的频带分割部分 11，其结构与现有技术中所描述的频带分割部分 11 的相同，因此，这里将部分地省略对其描述。

频带分割部分 11 接收数字化图象信号 71 并通过离散子波变换将图象信号

71 划分成 10 个频带中的信号，即 LL3 信号、LHi 信号、HLi 信号和 HHi 信号(i=1 至 3，下文同样如此)，计算每个信号中的子波系数。块分割部分 12 以预定尺寸对在频带分割部分 11 进行的分割所获得的频带中的待嵌入数字信息的频带(下文中称为嵌入目标区域)进行分割。密钥产生部分 13 利用预定函数从具有预定值的密钥产生一个二级密钥以及产生并存储表示是否把所产生二级密钥用于嵌入操作的密钥信息。能量分析部分 14 基于由密钥产生部分 13 所产生的二级密钥指定相应块，以及计算每个频率内的除嵌入目标区域之外的对应于与所指定块位置相同的空间表示区域的子波系数的能量。如果由能量计算部分 14 所计算的能量不小于预定的设定值 T，信息嵌入部分 15 将组成数字信息的比特之一嵌入到 LL3 信号中指定块的子波系数中。频带合成部分 16 将已经经过嵌入处理的 LL3 信号与其它频带中的信号相合成，重新构成一个图象信号 72。

现在参考图 2 至 5，一步步地描述由根据第一实施例的数字信息嵌入装置 1A 进行的数字信息嵌入方法。将通过示例描述嵌入目标区域是 LL3 信号(MRA 分量)和嵌入目标区域以外的频带是 MRR 分量的情况。

图 2 是由图 1 所示的块分割部分 12、密钥产生部分 13、能量分析部分 14 和信息嵌入部分 15 进行的处理的流程图。图 3 是通过分割 LL3 信号所获得的块的例子的图示。图 3 示出，在 LL3 信号被划分成 2×2 个块的情况中，第 x 个块的四个子波系数。图 4 示出表明存储是否采用二级密钥的密钥信息的表的例子。图 5 示出 LL 信号中的一个块与对应于同该块位置相同的空间表示区域的各 MRR 分量之间的位置关系。在以下的描述中，待嵌入在数字图象中的数字信息将是通过对版权持有人姓名、创作日期等进行二进制编码的获得的位流。

参考图 2，块分割部分 12 首先以预定块尺寸把由频带分割部分 11 输出的为嵌入目标区域的 LL3 信号分割成第一至第 N 个块(N 是不小于 2 的整数，下文同样如此)(步骤 S201)。通过分割所获得的块的数目 N 不小于待嵌入的数字信息的逻辑值的数目 Y。除图 3 所示的 2×2 尺寸以外，块的尺寸可以是任意尺寸，块的形状不必一定是正方形或长方形，可以是其它形状(例如，三角形和菱形)

然后，密钥产生部分 13 取代表组成待嵌入数字信息的信息的位的位置的计数 y(y 的取值在 1 至数字信息的最后位 Y 的范围内，下文中同样如此)的值为“1”(步骤 S202)。密钥产生部分 13 对存储密钥信息的表进行初始化(步骤 S203)，密钥信息用 “标志 0” 表示是否将二级密钥用于嵌入操作。在步骤

S209，把“标志 1”存储在表的对应于所采用二级密钥的部分中(即设定标志)，后面将描述。然后，密钥产生部分 13 利用预定函数 G 基于 y 的值计算初始值 r_0(步骤 S204)。函数 G 最好是这样设定的，即在 y=1 至 y=Y 的情况中，按照预定规则，将初始值 r_0取为彼此不同的整数。密钥产生部分 13 取计数 j(j=1 至 N，下文中相同)，用于把二级密钥指定为“1”(步骤 S205)。密钥产生部分 13 利用预定函数 F 从密钥 r_{j-1}产生二级密钥 r_j(步骤 S206)。函数 F 最好这样设定的，即按照预定规则每一个所产生的二级密钥 r_1至 r_N的取值在 1 至 N 的范围内。在第一流程中，密钥产生部分 13 从初始值密钥 r_0产生二级密钥 r_1。

然后，密钥产生部分 13 参考该表(存在或不存在“标志 1”)，判定在上述步骤 S206 所产生的二级密钥 r_j是否已经用于嵌入处理(步骤 S207)。在步骤 S207，当判定采用二级密钥 r_j时，密钥产生部分 13 在步骤 S206 使计数 j 的值增加 1，重复进行后续的步骤以便产生另一个二级密钥(步骤 S208)。另一方面，在上一步骤 S207，当判定未采用二级密钥 r_j时，密钥产生部分 13 通过将“标志 1”存储在表的相应部分中(设定标志)记录表示 r_j可被用于数字信息嵌入处理的信息(步骤 S209)(图 4)。通过处理，对于代表组成数字信息的第一至第 N 个位的各个信息，使不同的块经过嵌入处理。在第一流程中，“标志 1”未存储在表中，所以步骤 S207 的判定是“Yes”。

然后，能量分析部分 14 在以上步骤 S201 通过分割所获得的 LL3 信号(MRA 分量)的第一至第 N 块当中选择对应于二级密钥 r_j值的块(步骤 S210)。例如，当二级密钥 r_j的值是 x 时，能量分析部分 14 选择 LL3 信号中的第 x 个块(图 3)。在选择之后，能量分析部分 14 提取频带中的嵌入目标区域(即 MRR 分量)以外的对应于与所选块位置相同的空间表示区域的子波系数。对应于与 MRA 分量中块位置相同的空间表示区域的 MRR 分量中的子波系数意指 MRR 分量的每个分层中的信号，代表与 MRA 分量中块位置的象素相同的象素。在本发明中，最好是仅仅提取和使用更深分层信号中的子波系数。例如，在图 5 中，能量分析部分 14 提取总共 40 个象素，即为第三分层信号的 LH3 信号和 HL3 信号的 4 个象素，和作为第二分层信号的 LH2 信号和 HL2 信号的 16 个象素。

然后，能量分析部分 14 计算在以上步骤 S211 所提取的 MRR 分量中的子波系数的能量(步骤 S212)。用于能量计算的例如有寻找所提取子波系数的绝对幅度值之和的方法、寻找所提取子波系数的平方之和的方法、或者寻找所提取

子波系数的标准离差的方法。然后，信息嵌入部分 15 判定在上述步骤 S212 所计算的能量是否不小于预定的设定值 T(步骤 S213)。设定值 T 是判定数字信息的嵌入是否使图象质量几乎不降低的阈值。因此，设定值 T 不是唯一确定的，而是例如能够根据装置的用途和装置所处理的图象信号的水平适当地和任意地设定的。通过处理，嵌入处理能够仅针对不会极大地降低图象质量的块进行。

当在上述步骤 S213 判定能量不小于设定值 T 时，信息嵌入部分 15 将对应于子波系数中数字信息的第 y 位的信息(逻辑值)嵌入到 LL3 信号的所选块中(步骤 S214)。嵌入处理是利用上述嵌入方法(例如以前申请的专利)进行的。与此相反，当在上述步骤 S213 判定能量小于设定值 T 时，判定不应当将数字信息嵌入块中，计数 j 的值增加“1”，然后，重复进行步骤 S206 和后续的步骤的处理，以便产生另一个二级密钥(步骤 S208)。

在终止对应于第 y 位的信息的嵌入处理后，信息嵌入部分 15 判定数字信息是否已经被嵌入，即对应于第一至第 Y 位的信息的嵌入处理是否已经完成(步骤 S215)。当判定在步骤 S215 未完成对应于第一至第 Y 位的信息的嵌入处理时，信息嵌入部分 15 使计数 y 的值增加“1”，以便进行对应于接下来第 y+1 位的信息的嵌入处理(步骤 S216)。然后，过程返回到上述步骤 S204，重复进行相同处理。另一方面，当在上述步骤 S215 判定对应于第一至第 Y 位的信息被嵌入时，则终止嵌入处理。

参考图 6 和 7 描述由频带合成部分 16 进行的处理。简单地说，频带合成部分 16 进行的处理与由频带分割部分 11 所进行的处理相反。图 6 是表明图 1 所示频带合成部分 16 的详细结构的示例图。在图 6 中，频带合成部分 16 包括第一至第三频带合成滤波器 400、500 和 600，它们的结构相同。第一至第三频带合成滤波器 400、500 和 600 中的每一个接收四个频带信号，并对信号进行合成，输出一个信号。

第一频带合成滤波器 400 接收已经嵌入数字信息的 LL3 信号、LH3 信号、HL3 信号和 HH3 信号并将这些信息合成为一个 LL2 信号。第二频带合成滤波器 500 接收通过合成获得的 LL2 信号以及 LH2 信号、HL2 信号和 HH2 信号并将这些信号合成为一个 LL1 信号。第三频带合成滤波器 600 接收通过合成获得的 LL1 信号以及 LH1 信号、HL1 信号和 HH1 信号并将这些信号合成，重新构成一个图

象信号 72。

图 7 是表明图 6 所示的第一频带合成滤波器 400 的详细结构的示例图。在图 7 中，第一频带合成滤波器 400 包括第一至第三双频带合成部分 401 至 403，分别包括 LPF 411 至 413、HPF 421 至 423、以 2:1 的比例将零插入信号的上取样器 431 至 433 和 441 至 443 和加法器 451 至 453。

第一双频带合成部分 401 接收 LL3 信号和 LH3 信号，利用上取样器 431 至 441 分别将信号变换为尺寸为其原始尺寸两倍的信号，利用 LPF 411 和 HPF 421 针对它们的垂直分量对通过变换所获得的两个信号进行滤波，然后将信号相加，输出相加结果。另一方面，第二双频带合成部分 402 接收 HL3 信号和 HH3 信号，利用上取样器 432 至 442 分别将信号变换为尺寸为其原始尺寸两倍的信号，利用 LPF 412 和 HPF 422 针对它们的垂直分量对通过变换所获得的两个信号进行滤波，然后将信号相加，输出相加结果。第三双频带合成部分 403 接收加法器 451 和 452 的输出，利用上取样器 433 至 443 分别将信号变换为尺寸为其原始尺寸两倍的信号，利用 LPF 413 和 HPF 423 针对它们的水平分量对通过变换所获得的两个信号进行滤波，然后将信号相加，输出相加结果。

因此，从第一频带合成滤波器 400 输出 LL2 信号，它为第二分层信号，在其水平和垂直两个分量中均为低。第二和第三频带合成滤波器 500 和 600 按照如上所述，也针对向其输入的信号，分别进行同样处理。

频带合成部分 16 按照如上所述，对上述过程中的 10 个频带信号，即 LL3 信号、LHi 信号、HLi 信号和 HHi 信号进行合成，并重新构成已经经过嵌入处理的图象信号 72，输出重构的图象信号 72。

如上所述，在根据本发明第一实施例的数字信息嵌入装置 1A 中，采用组成待嵌入数字信息的信息位的位置作为密钥，利用预定函数产生二级密钥，判定频带中的嵌入目标区域以外的对应于与基于二级密钥所选块位置相同的空间表示区域的子波系数的能量，以嵌入数字信息。因此，在解码时使图象质量几乎不降低。不知道产生二级密钥方法的第三人几乎没有被嵌入数字信息的一点线索。

由根据第一实施例的数字信息嵌入装置 1A 进行的离散子波变换并不局限于三个分层。例如，能够进行多次直至 LL 信号达到 1×1 单元。在第一实施例的能量分析部分 14 中计算能量的方法并不局限于寻找子波系数绝对幅度值之

和的方法、寻找子波系数平方之和的方法以及寻找子波系数的标准离差的方法。例如，可以利用其它方法进行计算。尽管在第一实施例中，以利用标志作为表示是否采用二级密钥的密钥信息为例，但是并不是说不能采用另一种形式的信息，只要它能够代表存在或不存在二级密钥的使用。

在上述的第一实施例中，描述是针对嵌入目标区域是 LL3 信号(MRA 分量)(这是最低频带)和除嵌入目标区域以外的频带是除 MRA 分量以外的 MRR 分量的情况。然而，在与以上描述相同的过程中即使嵌入目标区域是 MRR 分量也能够根据本发明的数字信息进行嵌入处理。在这种情况中，可以采用频带(它在相对于其水平和垂直两个分量的带分割方向中与嵌入目标区域中的相同)中子波系数作为频带中的除嵌入目标区域以外的对应于相同空间表示区域(该区域被用于能量计算)的子波系数。例如，通过取嵌入目标区域作为 HL3 信号，使用 HL2 信号中子波系数(图 8)，而通过取嵌入目标区域为 HL2 信号，使用 HL3 信号中的子波系数。可以采用在频带中在相对于其水平和垂直两个分量的带分割方向上不同于嵌入目标区域中方向的子波系数作为上述子波系数。例如，通过取嵌入目标区域为 HL3 信号能够使用 LH3 信号中的子波系数（图 10）。

(第二实施例)

图 11 是表明根据本发明第二实施例的数字信息提取装置结构的方框图。根据第二实施例的数字信息提取装置 1B 是一个提取由根据上述第一实施例的数字信息嵌入装置 1A 嵌入的数字信息的装置。在图 11 中，根据第二实施例的数字信息提取装置 1B 包括频带分割部分 11、块分割部分 12、密钥产生部分 13、能量分析部分 14 和信息检测部分 21。

根据第二实施例的数字信息提取装置 1B 中的频带分割部分 11、块分割部分 12、密钥产生部分 13、能量分析部分 14 分别具有与根据第一实施例的数字信息嵌入装置 1A 中频带分割部分 11、块分割部分 12、密钥产生部分 13、能量分析部分 14 相同的结构，并指定了相同的参考标号，因此，将部分地省略对其的描述。

频带分割部分 11 接收图象信号 81。图象信号 81 是由根据第一实施例的数字信息嵌入装置 1A 中频带合成部分 16 输出的图象信号 72。频带分割部分 11 使接收的图象信号 81 经受离散子波变换，将图象信号 81 划分成 10 个频带中的信号，即 LL3 信号、LHi 信号、HLi 信号和 HHi 信号，计算每个信号中的

子波系数。如果能量分析部分 14 计算的能量不小于预定的设定值 T，那么信息检测部分 21 从 LL3 信号的指定块中的子波系数检测所嵌入的数字信息。

参考图 12，一步步地描述由根据第二实施例的数字信息提取装置进行的数字信息提取方法。现在描述对应于在数字信息嵌入装置中通过取嵌入目标区作为 LL3 信号（MRA 分量），取嵌入目标区域以外的频带作为 MRR 分量而进行嵌入处理的情况。图 12 是表明由图 11 所示的块分割部分 12、密钥产生部分 13、能量分析部分 14 和信息检测部分 21 进行处理的流程图。

参考图 12，块分割部分 12 首先以预定块尺寸将频带分割部分 11 输出的为嵌入目标区域的 LL3 信号分割成第一至第 N 个块(步骤 S1201)。密钥产生部分 13 然后取计数 y 的值为“1”(步骤 S1202)，计数 y 代表组成待嵌入数字信息的信息的位的位置。此外，密钥产生部分 13 对存储密钥信息的表进行初始化(步骤 S1203)，密钥信息通过“标志 0”表示是否采用二级密钥进行嵌入操作。然后，密钥产生部分 13 利用预定函数 G 基于 y 值计算初始值 r_0(步骤 S1204)。密钥产生部分 13 取计数 j 用于指令二级密钥的为“1”(步骤 S1205)。密钥产生部分 13 利用预定函数 F 从密钥 r_{j-1} 产生二级密钥 r_j(步骤 S1206)。

然后，密钥产生部分 13 参考该表，判定在上述步骤 S1206 所产生的二级密钥 r_j 是否已经被用于嵌入处理(步骤 S1207)。在步骤 S1207，当判定二级密钥 r_j 已被使用时，密钥产生部分 13 使计数 j 的值增加“1”，重复进行步骤 S1206 和后续的步骤的处理，以便产生另一个二级密钥(步骤 S1208)。另一方面，在上述步骤 S1207 中，当判定还未采用二级密钥 r_j 时，密钥产生部分 13 通过在表的相应部分中存储“标志 1”(设定标志)，记录表示二级密钥 r_j 被用于数字信息嵌入处理的信息(步骤 S1209)。

然后，能量分析部分 14 从在上述步骤 S1201 通过分割所获得的 LL3 信号(MRA 分量)中第一至第 N 块中选择对应于二级密钥 r_j 值的块(步骤 S1210)。选择之后，能量分析部分 14 提取该频带中的嵌入目标区域(即 MRR 分量)以外的对应于与所选块的位置相同的空间表示区域的子波系数(步骤 S1211)。正如第一实施例中所述的，能量分析部分 14 仅提取较深层次的第二和第三分层信号中的子波系数。能量分析部分 14 计算在上述步骤 S1211 已经提取的 MRR 分量中的子波系数(步骤 S1212)。

然后，信息检测部分 21 判定在上述步骤 S121 中计算的能量是否不小于预

定的设定值 T(步骤 S1213)。当在步骤 S1213 中判定能量不小于设定值 T 时，信息检测部分 21 从 LL3 信号所选块的子波系数中检测对应于被嵌入数字信息的第 y 位的信息(逻辑值)(步骤 S1214)。与此相反，当在步骤 S1213 中判定能量小于设定值 T 时，判定没有数字信息嵌入在该块中，计数 j 的值增加“1”，重复步骤 S1206 和后续的步骤，以便产生另一个二级密钥(步骤 S1208)。

在终止对应于第 y 位的信息的提取处理后，信息检测部分 21 判定是否已经提取了每一个数字信息，即是否已经进行了对应于第一至第 Y 位的信息的提取处理(步骤 S1215)。当在步骤 S1215 中判定，对应于第一至第 Y 位的信息的提取处理未完成时，信息检测部分 21 使计数 y 的值增加“1”，以便继续对应于接下来第 y+1 位的信息的提取处理(步骤 S1216)。尔后，程序返回到上述步骤 S1204，重复地进行相同处理。另一方面，当在步骤 S1215 中判定已经提取了对应于第一至第 Y 位的信息时，则终止提取处理。

因此，信息检测部分 21 针对组成数字信息的所有的位，进行上述的数字信息提取处理，分别地提取嵌入在图象信号 81 中的信息(逻辑值)，将信息重现为数字信息的位流 82。

如上所述，根据本发明第二实施例的数字信息提取装置 1B 采用组成被嵌入的数字信息的信息的位的位置作为密钥，利用预定函数产生二级密钥，判定频带中的嵌入目标区域以外的对应于与基于二级密钥所选块位置相同的空间表示区域的子波系数的能量，提取数字信息。因此，能够准确地提取数字信息，不受未经授权的用户尝试的影响。此外，不知道产生二级密钥方法的第三人几乎没有被嵌入数字信息的一点线索。

(第三实施例)

图 13 是示出依据本发明第三实施例的数字信息嵌入设备的结构的方框图。在图 13 中，依据第三实施例的数字信息嵌入设备 2A 包括频带分割部分 11、块分割部分 12、密钥产生部分 13、能量分析部分 14、系数倍乘部分 31、信息嵌入部分 15 和频带合成部分 16。依据第三实施例的数字信息嵌入设备 2A 中的频带分割部分 11、块分割部分 12、密钥产生部分 13、能量分析部分 14、信息嵌入部分 15 和频带合成部分 16 分别具有与依据第一实施例的数字信息嵌入设备 1A 中的频带分割部分 11、块分割部分 12、密钥产生部分 13、能量分析部分 14、信息嵌入部分 15 和频带合成部分 16 相同的结构，给这些部分指定相同的

标号，因而部分省略其描述。

如果能量分析部分 14 计算得到的能量在不小于预定设定值 T 但小于预定上限值 T1(T1≥T)的范围内，则系数倍乘部分 31 把用于能量计算的子波系数乘以预定值 U(U 为不小于 1 的实数)。另一方面，如果能量分析部分 14 计算得到的能量在小于预定设定值 T 但不小于预定下限值 T2(T2≤T)的范围内，则系数倍乘部分 31 把用于能量计算的子波系数乘以预定值 L(L 为不超过 1 的实数)。如果能量不小于预知设定值 T，则信息嵌入部分 15 把构成数字信息的位之一嵌入到嵌入目标区域中的指定块的子波系数中。频带合成部分 16 合成嵌入目标区域中经过嵌入处理的信号与嵌入目标区域以外的多个频带中的信号，以重构图象信号 73。

参考图 14 和 2，分步描述由依据第三实施例的数字信息嵌入设备 2A 所执行的数字信息嵌入方法。图 14 是示出由图 13 所示的块分割部分 12、密钥产生部分 13、能量分析部分 14、系数倍乘部分 31 和信息嵌入部分 15 所进行的处理的流程图。在图 14 中，给进行与图 2 所示相同处理的步骤指定与图 2 所示相同的步骤标号，因而不重复其描述。

参考图 14，能量分析部分 14 根据密钥产生部分 13 产生的二级密钥 r_j 而选中对应的嵌入目标区域中的一个块，即 LL3 信号(步骤 S210)。提取对应于与该块位置相同的空间表象区域的每个 MRR 分量(它们是嵌入目标区域以外的多个频带)中的子波系数(步骤 S211)。能量分析部分 14 计算 MRR 分量中所提取的子波系数的能量(步骤 S212)。

然后，系数倍乘部分 31 判断上述步骤 S212 处计算得到的能量是否小于预定设定值 T(步骤 S213)。当在步骤 S213 判定能量不小于设定值 T 时，系数倍乘部分 31 进一步判断上述步骤 S212 处计算得到的能量是否不超过预定上限值 T1(步骤 S1401)。当在步骤 S1401 判定能量不超过预定上限值 T1 时，系数倍乘部分 31 把在上述步骤 S211 处提取的 MRR 分量中的所有子波系数都乘以 U(步骤 S1402)。其后，信息嵌入部分 15 把对应于数字信息中第 y 位的信息(逻辑值)嵌入 LL3 信号的选中块的子波系数中(步骤 S214)。与此相反，当在上述步骤 S1401 判定能量超过上限值 T1，则信息嵌入部分 15 把对应于数字信息中第 y 位的信息(逻辑值)嵌入 LL3 信号的选中块的子波系数中，而不在系数倍乘部分 31 中把子波系数乘以 U(步骤 S214)。

另一方面，当在上述步骤 S213 判定能量小于设定值 T，则系数倍乘部分

31 进一步判断在上述步骤 S212 处计算得到的能量是否不小于预定下限值 T2(步骤 S1403)。当在步骤 S1403 判定能量不小于下限值 T2，则系数倍乘部分 31 把在上述步骤 S211 处提取的 MRR 分量中的所有子波系数乘以 L(步骤 S1404)。其后，把计数器 j 的值递增“1”，为产生另一个二级密钥而重复步骤 S206 及随后步骤的处理(步骤 S208)。与此相反，当在上述步骤 S1403 判定能量小于下限值 T2，则计数器 j 的值递增“1”，且为产生另一个二级密钥而重复步骤 S206 及随后步骤的处理，而不在系数倍乘部分 31 中把子波系数乘以 L(步骤 S208)。

以下描述这样一个例子，其中把对应于与图 3 所示块位置相同的空间表象区域的每个 MRR 分量中的子波系数乘以 U。在本例中，由子波系数的绝对幅值的和来计算能量。设定值 T 取作 130，上限值 T1 取作 140，U 取作 1.1。

当 MRR 分量中的子波系数如下时，在步骤 S211 处提取的 MRR 分量中的子波系数的能量为 133：

HL3={10, -5, 1, -2}

LH3={0, 2, -3, 7}

HL2={1, 3, -2, 6, 9, 12, -20, -16, 4, 8, 1, -2, -3, 1, 0, 1}

LH2={2, 1, 0, -1, -2, 0, 1, 1, 0, -1, -3, 0, 0, 1, -1, 0}

结果，能量不小于设定值 T 也不超过上限值 T1。因而，本例中 MRR 分量中的子波系数分别乘以 U，并由以下子波系数来替换(此时，MRR 分量中子波系数的能量为 146.3)：

HL3={11, -5.5, 1.1.-2.2}

LH3={0, 2.2, -3.3, 7.7}

HL2={1.1, 3.3, -2.2, 6.6, 9.9, 13.2, -22, -17.6, 4.4, 8.8, 1.1, -2.2, -3.3, 1.1, 0, 1.1}

LH2={2.2, 1.1, 0, -1.1, -2.2, 0, 1.1, 1.1, 0, -1.1, 0, -1.1, -3.3, 0, 0, 1.1, -1.1, 0}

如上所述，在依据本发明第三实施例的数字信息嵌入设备 2A 中，把构成待嵌入数字信息的信息的位的位置用作密钥以利用预定函数产生二级密钥，并判断对应于与根据二级密钥选中的块的位置相同的空间表象区域的每个频带(嵌入目标区域以外)中的子波系数的能量，以嵌入该数字信息。结果，图象的质量在解码时几乎没有降低，且不知道二级密钥产生方法的第三人对嵌入的数

字信息没有线索。

此外，在依据本发明第三实施例的数字信息嵌入设备中，只有当对应于与选中块的位置相同的空间表象区域的多个频带(嵌入目标区域以外)中每一个频带(即 MRR 分量)中的子波系数的能量接近于设定值 T 时，才把子波系数与预定值倍乘(U 或 L)。因此，在数字信息提取处理中，与依据第一实施例的数字信息嵌入设备 1A 相比，可在能量不小于设定值 T 的情况下，更令人满意地防止错误检测和不完全检测以防止第三人未经许可地利用(例如，图象压缩)。因而，可准确地提取嵌入的数字信息。

依据第一到第三实施例的数字信息嵌入设备和提取设备中所使用的数字图象信号不限于静止图象信号。例如，它可以是活动图象信号。在活动图象信号的情况下，通过对构成活动图象(例如，每秒每 30 个帧)的每个帧进行数字信息的嵌入处理和提取处理可产生相同的效果。在依据第一到第三实施例的数字信息嵌入设备和提取设备中，利用能量分析部分 14 来分析能量，且数字信息只嵌入包括其能量不小于设定值 T 的子波系数的块中。然而，不用说，可不进行分析处理而嵌入数字信息。

(第四实施例)

在第一到第三实施例中，对嵌入和提取对应于一图象信号的细部的 MRA 分量或较低频带中的 MRR 分量中的数字信息的设备和方法进行了描述。与此相反，在以下的实施例中，将描述利用来自每个低频分量(除 DC 分量以外)的频率系数中的多个频率系数的平均值来嵌入和提取数字信息的设备和方法。

图 15 是示出依据本发明第四实施例的数字信息嵌入设备的结构的方框图。在图 15 中，依据第四实施例的数字信息嵌入设备 3A 包括块分割部分 41、频率变换部分 42、系数计算部分 43、量化部分 44、信号替换部分 45、系数修正部分 46 和频率逆变换部分 47。

块分割部分 41 接收数字化图象信号 74，并把图象信号 74 分割成具有预定块尺寸的多个块。频率变换部分 42 对通过块分割部分 41 的分割而获得的每个块进行频率变换，以计算频率系数 C。系数计算部分 43 从频率变换部分 42 获得的频率系数中选中多个特定频率系数 C 来计算选中频率系数 C 的绝对值的平均值(以下叫做绝对平均值)M 和所选频率系统 C 的能量 S。量化部分 44 使找到的绝对平均值经过线性量化，仅当系数计算部分 43 找到的能量 S 不小于预定阈值 K 时，利用预定量化步长 Q 来计算量化值 q。信号替换部分 45 以值(q-1)

或值(q+1)来替换量化值 q 输出，或者根据量化值 q 和待嵌入的数字信息的值来输出值 q。系数修正部分 46 使信号替换部分 45 输出的量化值(q-1)或(q+1)或量化值 q 经过逆线性量化，以利用量化步长 Q 而找到平均值 M′并计算平均值 M′与绝对平均值 M 之间的差 DM(=M′-M)，以修正所有选中的频率系数 C。频率逆变换部分 47 使通过块分割部分的分割而获得的所有块分别经过频率逆变换，以重构图象信号 75。

现在参考图 16 到 18，分步描述依据本发明第四实施例的数字信息嵌入设备 3A 所执行的数字信息嵌入方法。图 16 是示出块分割部分 41 和频率变换部分 42 所进行的处理的一个例子的图。图 17 是示出图 15 所示的系数计算部分 43、量化部分 44、信号替换部分 45 和系数修正部分 46 所进行的处理的流程图。图 18 是示出图 15 所示的信号替换部分 45 所进行的处理的一个例子的图。在以下描述中，待嵌入数字图象的数字信息应为通过对版权持有者的名称、生产日期等进行二进制编码而获得的位流。

参考图 16，块分割部分 41 首先接收数字图象信号 74，并把数字图象信号 74 分割成具有预定块尺寸的第一到第 N(N 为不小于二的整数；下同)块。通过分割所获得的块的数目 N 不小于待嵌入的数字信息的逻辑值的数目。然后，频率变换部分 42 对通过块分割部分 41 的分割而获得的第一到第 N 块中的每个信号进行频率变换，以计算相同块尺寸的频率系数 C。

图 16 示出在块分割部分 41 和频率变换部分 42 中，把图象信号 74 分割成多个块，每个块 8×8 的像素构成(图 16(a))，每个块经过离散余弦变换(DCT)的正交变换(从图 16(b)到图 16(c))。图 16(c)所示频率系数中左上方的频率系数 C 指 DC 分量(DC)，其它频率系数 C 指 AC(交流)分量。块尺寸可以是不同于图 16 所示 8×8 的任意尺寸。

参考图 17，系数计算部分 43 首先把代表通过块分割部分 41 的分割而获得的块的位置的计数 n(n=1 到 N；下同)的值取作“1”(步骤 S1701)。然后，系数计算部分 43 从频率变换部分 42 中找到的第 n 个块的多个频率系数 C 中选中特定频率系数 C_1 到 C_a(a 为不小于 1 的整数)(步骤 S1702)。这里把选中的频率系数 C_1 到 C_a 的组叫做频率系数串(string)Ca。在本发明中，最好选中较接近 DC 分量的低频分量中的频率系数串 Ca。例如，在图 16(c)所示的例子中，选中由 DC 分量(由图中实线所包围的部分)附近的九个频率系数 C_1 到 C_9 构成的频率系数串 C9。

此外，系数计算部分 43 计算选中频率系数串 Ca 的绝对平均值 M 和能量 S(步骤 S1703)。例如，利用找到构成频率系数串 Ca 的频率系数 C_1 到 C_n 的绝对幅值的和或平均值的方法、找到其平方的和或平均值的方法或找到标准离差的方法来计算能量 S。

然后，量化部分 44 判断在上述步骤 S1703 处计算得到的能量 S 是否不小于预定阈值 K(步骤 S1704)。阈值 K 为判断嵌入数字信息是否降低图象质量的值。结果，阈值 K 并非唯一地确定，而可依据设备用途或设备所操纵的图象信号的水平等而适当地任意设定。通过该处理，可只对未大大降低图象质量的块进行嵌入处理。

当在上述步骤 S1704 处判定能量 S 不小于阈值 K 时，使绝对平均值 M 经过线性量化，以利用预定量化步长 Q(Q 为不小于一的整数)来计算量化值 q(步骤 S1705)。“线性量化”指通过依据舍入规则对某一数值的小数点后的数字进行上舍入或下舍入而把该数值四舍五入成整数(函数 int[X]应代表 X 的线性量化)。量化步长 Q 为把待嵌入数字信息取作逻辑值“1”的情况下的变换值与把它取作逻辑值“0”的情况下的变换值之间的间隔或替换量。因此，当量化步长减小时，图象的质量几乎不降低，而数字信息的防范企图能力下降。当量化步长 Q 增大时，数字信息的防范企图能力增强，而图象质量因替换量的增大而明显降低。结果，量化步长 Q 并非唯一地确定，而可根据用途和目标图象信号而任意设定。在本发明第四实施例的描述中，量化步长 Q 取作 10。

例如，当频率系数串 C9 如下时，在上述步骤 S1703 处选中的频率系数串 C9 的绝对平均值 M 为 31(=279/9)：

C9={80, -60, 45, 20, -25, 20, 10, -10, 9}

结果，如上所述，量化值 q 如下，

q=int[M/Q]=int[31/10]=3

另一方面，当在上述步骤 S1704 判定能量 S 小于阈值 K，则判定不应把数字信息嵌入第 n 个块。为了指定随后的块，把计数 n 的值递增“1”(步骤 S1719)，重复步骤 S1702 及随后步骤的处理。

然后，信号替换部分 45 提取待嵌入第 n 个块的数字信息的逻辑值(“1”或“0”)(步骤 S1706)。其后，信号替换部分 45 判断量化值 q 为偶数还是奇数(步骤 S1707)。

当在上述步骤 S1707 的判断中判定量化值 q 为偶数时，信号替换部分 45

进一步判断在上述步骤 S1706 处提取的数字信息的逻辑值是否为“1”(步骤 S1708)。当在步骤 S1708 判定待嵌入的逻辑值为“1”，则信号替换部分 45 把最接近 M/Q 的值的奇数(q+1 或 q-1)取作量化值 q′(即，以 q′来替换量化值 q)(步骤 S1710)。与此相反，当在上述步骤 S1708 判定待嵌入的逻辑值为“0”时，信号替换部分 45 把量化值 q 取作量化值 q′(步骤 S1712)。

另一方面，当在上述步骤 S1707 的判断中判定量化值 q 不是偶数(即，奇数)，则信号替换部分 45 进一步判断待嵌入的逻辑值是否为“0”(步骤 S1709)。当在步骤 S1709 判定待嵌入的逻辑值为“0”时，信号替换部分 45 把最接近 M/Q 的值的偶数(q+1 或 q-1)取作量化值 q′(步骤 S1711)。与此相反，当在上述步骤 S1709 判定待嵌入的逻辑值为“1”时，信号替换部分 45 把量化值 q 取作量化值 q′(步骤 S1712)。

例如，参考图 18，当绝对平均值 M 为 31 且量化步长 Q 为 10 时，量化值 q 为奇数“3”，M/Q 为 3.1。因此，通过沿行步骤 S1707 到 S1712，当嵌入数字信息的逻辑值“1”时，把 q=3 的值取作量化值 q′=3，因为量化值 q 为奇数。与此相反，当嵌入数字信息的逻辑值“0”时，把最接近 M/Q=3.1 的值的偶数即“4”取作量化值 q′(=q+1)。

然后，系数修正部分 46 在上述步骤 S1710 到 S1712 中任一个步骤处找到的量化值 q′和量化步长来进行逆线性量化，以计算平均值 M′(=q′×Q)(步骤 S1713)。系数修正部分 46 找到计算得到的平均值 M′与在上述步骤 S1703 处找到的绝对平均值 M 之间的差 DM(=M′-M)(步骤 S1714)。

此外，系数修正部分 46 判断在上述步骤 S1702 处选中的频率系数串 Ca 的符号是正还是负(步骤 S1715)。对频率系数串 Ca 的符号的判断指判断构成频率系数串 Ca 的频率系数 C_1 到 C_n 的各个符号的判断。当在上述步骤 S1715 的判断中频率系数 C_x 的符号为正(包括零)时，系数修正部分 46 把差 DM 加到每个频率系数 C_1 到 C_n(步骤 S1716)，而当频率系数 C_x 的符号为负时从中减去差 DM(步骤 S1717)，以找到修正后的频率系数串 Ca′。

例如，如上所述，在待嵌入的逻辑值为“0”的情况下，当在上述步骤 S1703 处选中的频率系数串 C9 如下时，q′=4：

C9={80, -60, 45, 20, -25, 20, 10, -10, 9}

因而，逆线性量化后的平均值 M′如下：

M′=q′×Q=4×10=40

平均值 M′与绝对平均值之间的差如下：

DM=M′-M=40-31=+9

结果，通过把“9”加到其值为正的频率系数 C，而把其值为负的频率系数 C 减去“9”的修正频率系数串 C9′如下，从而其绝对值大了“9”：

C9′={89, -69, 54, 29, -34, 29, 19, -19, 18}

在上述步骤 S1717 中，当差 DM 的值为负且频率系数 C_x 的绝对值小于差 DM 的绝对值时，产生这样的现象，即修正后的频率系数 C_x' 的绝对值并不小于而是大于修正前的频率系数 C_x 的绝对值。一个例子是这样的情况，其中差 DM 为-9，频率系数 C_x 为 3。修正后的频率系数 C_x' 为“-6”。在上述情况下，系数修正部分 46 通过把频率系数 C_x' 取作零来进行修正，以使发生误差的次数尽可能小。

即使频率系数串 Ca 的绝对平均值 M 不小于阈值 K，则当替换获得的量化值 q′等于值 K/Q 时，在系数修正部分 46 中进行逆线性量化时找到的平均值 M′如下：

$M'=q'\times Q=(K/Q)\times Q=K$

如此修正平均值 M′，从而修正后频率系数串 Ca′的绝对平均值变为阈值 K。

在上述情况下，系数修正部分 46 把预定设定值加到差 DM(=M′-M=K-M≤0)的值中，以如此改变差 DM 的值，使绝对平均值 M 大于阈值 K。

系数计算部分 43、量化部分 44、信号替换部分 45 和系数修正部分 46 判断是否已针对所有的第一到第 N 块进行了上述数字信息嵌入处理(上述步骤 S1702 到 S1717)(步骤 S1718)。当在步骤 S1718 判定还未在第一到第 N 块中进行数字信息的嵌入处理时，把计数 n 的值递增“1”，以继续随后的第(n+1)块中的数字信息的嵌入处理(步骤 S1719)。其后，程序返回上述步骤 S1702，以重复地进行同一处理。另一方面，当在上述步骤 S1718 处判定已在第一到第 N 块中进行了数字信息的嵌入处理，则嵌入处理终止。当数字信息嵌入处理终止时，频率逆变换部分 47 使所有的块分别经过频率逆变换(从图 16(c)到 16(b)的 IDCT)，以重构其中已嵌入数字信息的图象信号 75。

当构成数字信息的位数小于通过分割获得的块的数目时，可使用这样的方法，诸如嵌入构成数字信息的所有位然后以第一位开始连续地嵌入这些位的方法，以及在剩余的所有块中嵌入位“0(或 1)”的方法。或者，可把同一位嵌入几个块中。

如上所述，依据本发明第四实施例的数字信息嵌入设备 3A，判断 DC 分量

附近的低频分量中的频率系数串 Ca 的能量 S，以嵌入数字信息。结果，图象的质量在解码时几乎不降低，且可防止嵌入的数字信息和丢失，从而防止第三人的未经许可的利用。

依据第四实施例的数字信息嵌入设备 3A 中的频率变换部分 42 不限于上述离散余弦变换(DCT)。例如，可进行傅里叶变换或 Hadamard 变换。系数计算部分 43 中的特定频率系数串 Ca 的选择方法不限于较接近 DC 分量的低频分量中的九个频率系数 C_1 到 C_9。例如，可使用多个(不同于九个)频率系数。或者，不可以对每个块选中同一位置的频率系数 C。能量 S 的计算方法不限于找到频率系数串 Ca 的绝对幅值的和或平均值的方法、找到其平方的和或平均值的方法以及找到标准离差的方法。可使用其它方法进行计算。此外，信号替换部分 45 中的量化值 q 的替换处理可以这样的方式进行，使当待嵌入的数字信息的逻辑值为“0”时以最接近 M/Q 的值的奇数量化值来替换量化值 q，而当逻辑值为“1”时以最接近 M/Q 的值的偶数量化值来替换。

(第五实施例)

图 19 是示出依据本发明第五实施例的数字信息提取设备的结构的方框图。依据第五实施例的数字信息提取设备 3B 是提取由上述依据第四实施例的数字信息嵌入设备 3A 嵌入的数字信息的设备。在图 19 中，依据第五实施例的数字信息提取设备 3B 包括块分割部分 41、频率变换部分 42、系数计算部分 43、量化部分 44 和信息提取部分 51。

依据第五实施例的数字信息提取设备 3B 中的块分割部分 41、频率变换部分 42、系数计算部分 43 和量化部分 44 分别具有与依据第四实施例的数字信息嵌入设备 3A 中的块分割部分 41、频率变换部分 42、系数计算部分 43 和量化部分 44 相同的结构，并给这些部分指定相同的标号，因而部分省略其描述。

块分割部分 41 接收图象信号 83。除了依据第四实施例的数字线性嵌入设备 3A 中的频率逆变换部分 47 输出的图象信号 75 以外，图象信号 83 还包括在量化部分 44 中所使用的阈值 K 和用于线性量化的量化步长 Q。块分割部分 41 把接收到的图象信号 83 分割成具有预定块尺寸的多个块。频率变换部分 42 对通过分割而获得的每个块进行频率变换，以计算频率系数 C。系数计算部分 43 从频率变换部分 42 中获得的频率系数中选中多个特定频率系数 C，来计算所选频率系数 C 的绝对平均值 M 和能量 S。量化部分 44 使找到的绝对平均值 M 经过线性量化，以在系数计算部分 43 找到的能量 S 不小于预定阈值 K 时，利用预

定量化步长 Q 来计算量化值 q。信息提取部分 51 判断在量化部分 44 中计算得到的每个量化值 q 是偶数还是奇数，以此判断为基础来判断嵌入的数字信息的逻辑值。

现在参考图 20，分步描述依据本发明第五实施例的数字信息提取设备 3B 所执行的数字信息提取方法。图 20 是示出图 19 所示系数计算部分 43、量化部分 44 和信息提取部分 51 所进行的处理的流程图。

系数计算部分 43 首先把代表通过块分割部分 41 的分割而获得的块的位置的计数 n 的值取作“1”(步骤 S2001)。然后，系数计算部分 43 从频率变换部分 42 中找到的第 n 个块的频率系数 C 中选中特定频率系数 C_1 到 C_a，即频率系数串 Ca(步骤 S2002)。数字信息嵌入设备 3A 将图象信号 83 与代表频率系数串 Ca 的信息一起馈送。或者数字信息提取设备 3B 可预先固定地具有该信息。此外，系数计算部分 43 计算选中频率系数串 Ca 的绝对平均值 M 和能量 S(步骤 S2003)。

然后，量化部分 44 判断在上述步骤 S2003 处计算得到的能量 S 是否不小于给定的阈值 K(步骤 S2004)。当在上述步骤 S2004 处判定能量 S 不小于阈值 K 时，使绝对平均值 M 经过线性量化，以利用给定的量化步长 Q 来计算量化值 q(步骤 S2005)。与此相反，当在上述步骤 S2004 判定能量 S 小于阈值 K 时，则判定不把数字信息嵌入第 n 个块。为了指定随后的块，把计数 n 的值递增“1”(步骤 S2010)，重复步骤 S2002 及随后步骤的处理。

然后，信号提取部分 51 判断在上述步骤 S2005 处计算得到的量化值 q 为偶数还是奇数(步骤 S2006)。当在上述步骤 S2006 的判断中判定量化值 q 为偶数时，信号提取部分 51 判断已嵌入第 n 个块的数字信息的逻辑值是“0”(步骤 S2007)。另一方面，当在上述步骤 S2006 处判定量化值 q 为奇数时，则信号提取部分 51 判断已嵌入第 n 个块的数字信息的逻辑值是“1”(步骤 S2008)。

为了对第一到第 N 个所有的块进行上述数字信息提取过程(上述步骤 S2002 到 S2008)，信息提取部分 51 判断是否已对所有的块进行了处理(步骤 S2009)。当在步骤 S2009 判定还未对第一到第 N 块中的数字信息进行提取处理时，把计数器 n 的值递增“1”，以继续随后的第(n+1)块中的数字信息的提取处理(步骤 S2010)。其后，程序返回上述步骤 S2002，以重复地进行同一处理。另一方面，当在上述步骤 S2009 处判定已在第一到第 N 块中进行了数字信息的提取处理，则提取处理终止。

信息提取部分 51 如此对第一到第 N 所有的块进行上述数字信息提取处理，即分别提取嵌入图象信号中的逻辑值，并把这些逻辑值再现为数字信息的位流 84。

如上所述，在依据本发明第五实施例的数字信息提取设备 3B 中，由提取较低频率分量(几乎不受高频频带中的数据破坏的影响)中多个频率系数C并使用预定方法从这些频率系数 C 的绝对平均值 M 中计算量化值 q 的结果来判断嵌入的数字信息的逻辑值。结果，可提取正确的数字信息而不会受到未经许可的用户的尝试的影响。

(第六实施例)

图 21 是示出依据本发明第六实施例的数字信息嵌入设备的结构的方框图。在图 21 中，依据第六实施例的数字信息嵌入设备 4A 包括块分割部分 41、频率变换部分 42、系数计算部分 43、系数倍乘部分 61、量化部分 44、信号替换部分 45、系数修正部分 46 和频率逆变换部分 47。

依据第六实施例的数字信息嵌入设备 4A 中的块分割部分 41、频率变换部分 42、系数计算部分 43、量化部分 44、信号替换部分 45、系数修正部分 46 和频率逆变换部分 47 分别具有与依据第四实施例的数字信息嵌入设备 3A 中的块分割部分 41、频率变换部分 42、系数计算部分 43、量化部分 44、信号替换部分 45、系数修正部分 46 和频率逆变换部分 47 相同的结构，并给这些部分指定相同的标号，因而部分省略其描述。

块分割部分 41 接收数字化图象信号 74，并把图象信号 74 分割成具有预定块尺寸的多个块。频率变换部分 42 对通过块分割部分 41 的分割而获得的每个块进行频率变换，以计算频率系数 C。系数计算部分 43 从频率变换部分 42 获得的频率系数 C 中选中多个特定频率系数 C 来计算选中频率系数 C 的绝对值的平均值(绝对平均值)M 和能量 S。如果系数计算部分 43 计算得到的能量 S 在小于预定阈值 K 但不小于预定下限值 K1(K1≤K)的范围内，则系数倍乘部分 61 把用于计算能量 S 的频率系数串 Ca 乘以预定值 L(L 为不超过 1 的实数)。量化部分 44 使找到的绝对平均值 M 经过线性量化，仅当系数计算部分 43 找到的能量 S 不小于预定阈值 K 时，利用预定量化步长 Q 来计算量化值 q。信号替换部分 45 以值(q-1)或值(q+1)来替换量化值 q 输出，或者根据量化值 q 和待嵌入的数字信息的值来输出值 q。系数修正部分 46 使信号替换部分 45 输出的量化值(q-1)或(q+1)或量化值 q 经过逆线性量化，以利用量化步长 Q 而找到平均值

M′并计算平均值 M′与绝对平均值 M 之间的差 DM(=M′-M)，以修正所有选中的频率系数 C。频率逆变换部分 47 使通过块分割部分 41 的分割而获得的所有块分别经过频率逆变换，以重构图象信号 76。

现在参考图 22 和 17，分步描述依据本发明第六实施例的数字信息嵌入设备 4A 所执行的数字信息嵌入方法。图 22 是示出图 21 中所示的系数计算部分 43、系数倍乘部分 61、量化部分 44、信号替换部分 45 和系数修正部分 46 所进行的处理的流程图。在图 22 中，给与图 17 中所示步骤的处理相同的步骤分配与图 17 中所示相同的步骤标号，因而，不重复其描述。

参考图 22，系数计算部分 43 对于通过块分割部分 41 的分割而获得的多个块，从频率变换部分 42 中找到的第 n 个块的多个频率系数 C 中选中特定频率系数 C_1 到 C_a，即频率系数串 Ca(步骤 S1702)。系数计算部分 43 计算选中频率系数串 Ca 的绝对平均值 M 和能量 S(步骤 S1703)。

然后，系数倍乘部分 61 判断上述步骤 S1703 处计算得到的能量 S 是否不小于预定阈值 K(步骤 S2201)。当在步骤 S2201 判定能量不小于阈值 K 时，为把数字信息嵌入第 n 个块，继续进行上述步骤 S1705 及随后步骤的处理。另外，当在上述步骤 S2201 判定能量 S 小于阈值 K，则系数倍乘部分 61 进一步判断上述步骤 S1703 处计算得到的能量 S 是否不小于预定下限值 K1(步骤 S2202)。

当在上述步骤 S2202 判定能量 S 不小于下限值 K1，则系数倍乘部分 61 把构成在上述步骤 S1702 处选中的频率系数串 Ca 的每个频率系数 C_1 到 C_a 乘以 L(步骤 S2203)。当在上述步骤 S2202 判定能量 S 小于下限值 K1，且在上述步骤 S2203 把频率系数串 Ca 乘以 L 后，把计数 n 的值递增“1”，以继续随后第(n+1)个块中的数字信息的嵌入处理(步骤 S1719)。其后，程序返回上述步骤 S1702，以重复地进行同一处理。

以下示出这样一个例子，其中把图 16(c)中所示的频率系数串 C9 乘以 L。在本例中，作为频率系数串 C9 的绝对幅值的平均值来计算能量 S。把阈值 K 取作 20，下限值 K1 和 L 分别取作 15 和 0.9。

当频率系数串 C9 如下时，在上述步骤 S1702 处选中的频率系数串 C9 的能量 S 为 18.9(=170/9)：

C9={40, -40, 50, 20, -7, 5, -4, 3, 1}

结果，能量小于阈值 K 但不小于下限值 K1。因此，对于本例中的频率系数串 C9，把频率系数 C_1 到 C_a 分别乘以 L，并以以下频率系数串 C9 来替换：

C9={36, -36, 45, 18, -6.3, 4.5, -3.6, 2.7, 0.9}

(此时，替换后的频率系数串 C9 的能量 S 为 17(=153/9))。

如上所述，依据本发明第六实施例的数字信息嵌入设备 4A，判断 DC 分量附近的低频分量中的频率系数串 Ca 的能量 S 来嵌入数字信息。结果，图象的质量在解码时几乎不降低，且可防止嵌入的数字信息的丢失，防止第三人的未经许可的利用的尝试。

此外，在依据本发明第六实施例的数字信息嵌入设备 4A 中，只有当选中频率系数串 Ca 的能量 S 接近于阈值 K(实际上在稍小于 K 时)时，才把频率系数串 Ca 与预定值 L 倍乘。结果，在数字信息提取处理中，与依据第四实施例的数字信息嵌入设备 3A 相比，无论能量是否小于阈值 K，更令人满意地防止错误检测和不完全检测以防止第三人未经许可地利用。因而，可更准确地提取嵌入的数字信息。

依据第四到第六实施例的数字信息嵌入设备和提取设备中所使用的数字图象信号不限于静止图象信号。例如，它可以是活动图象信号。在活动图象信号的情况下，通过对构成活动图象(例如，每秒每 30 个帧)的每个帧进行数字信息的嵌入处理和提取处理可产生相同的效果。在依据第四到第六实施例的数字信息嵌入设备和提取设备中，利用系数计算部分 43 来计算能量 S，且数字信息只嵌入包括其能量不小于阈值 K 的子波系数的块中。然而，不用说，可不进行阈值处理而嵌入数字信息。

通常，通过用于存储预定程序数据的存储装置(ROM、RAM、硬盘等)和用于执行程序数据的 CPU(中央处理器)来实现依据第一到第六实施例的数字信息嵌入设备和提取设备所实现的每个功能。在此情况下，可通过诸如 CD-ROM 或软盘等记录媒体来引入每个程序数据。

虽然已详细地描述了本发明，但上述描述都是示意性的而不是限制性的。因此可以理解，能进行大量其它的修改和变化而不背离本发明的范围。

说 明 书 附 图

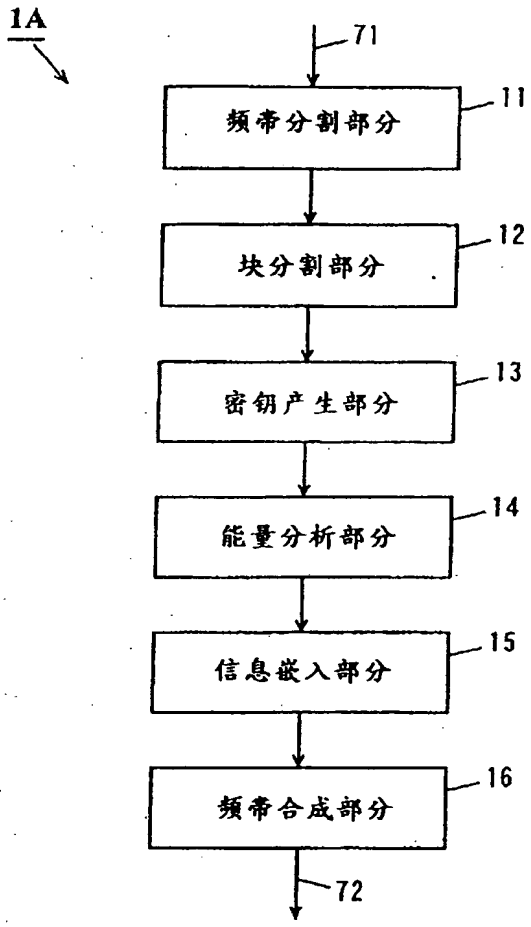

1A
71
频带分割部分
11
块分割部分
12
密钥产生部分
13
能量分析部分
14
信息嵌入部分
15
频带合成部分
16
72

图 1

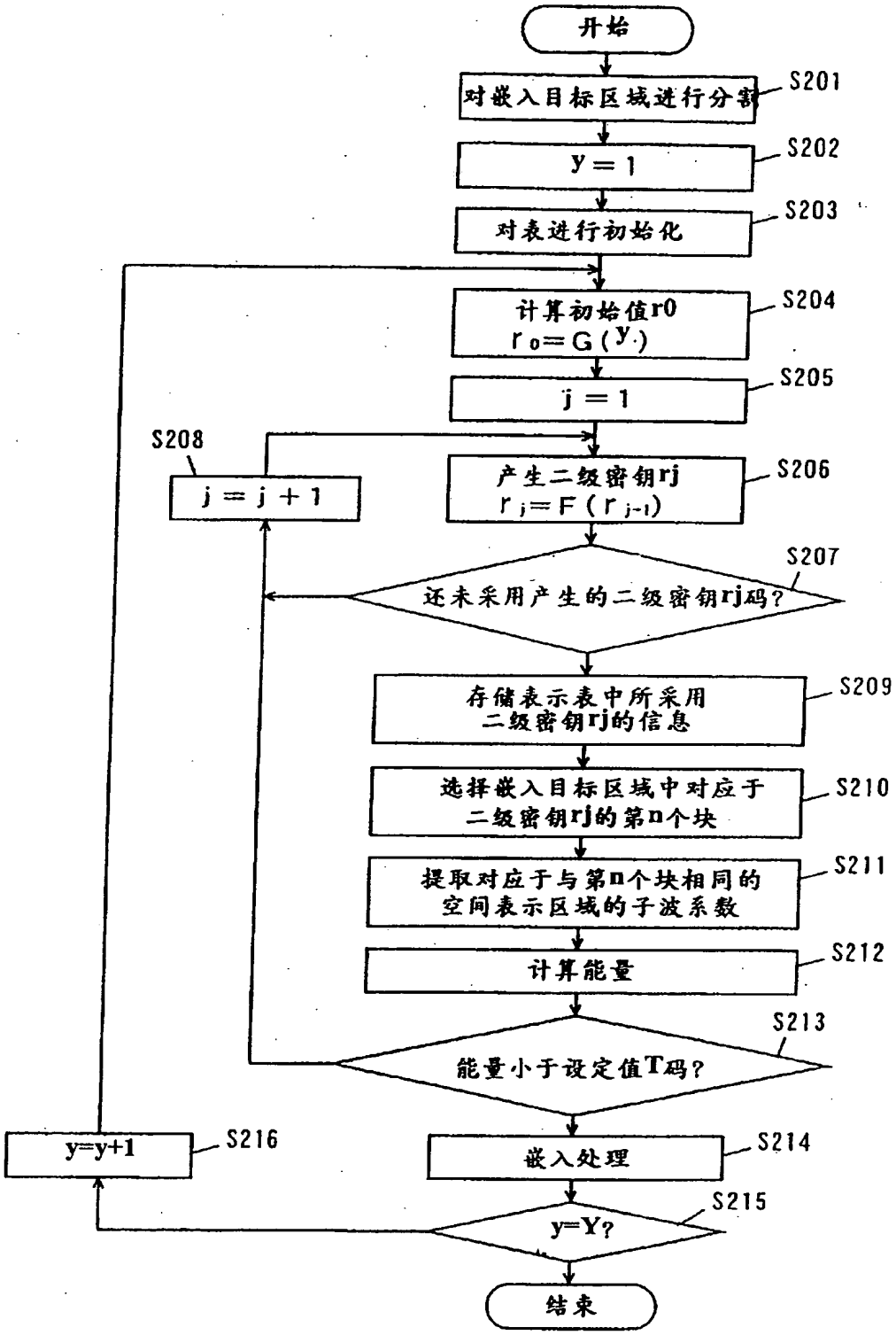

开始
对嵌入目标区域进行分割
S201
y＝1
S202
对表进行初始化
S203
计算初始值r0
r0＝G(y)
S204
j＝1
S205
S208
j＝j＋1
产生二级密钥rj
rj＝F(rj-1)
S206
S207
还未采用产生的二级密钥rj码?
存储表示表中所采用
二级密钥rj的信息
S209
选择嵌入目标区域中对应于
二级密钥rj的第n个块
S210
提取对应于与第n个块相同的
空间表示区域的子波系数
S211
计算能量
S212
S213
能量小于设定值T码?
y=y+1
S216
嵌入处理
S214
S215
y=Y?
结束

图　2

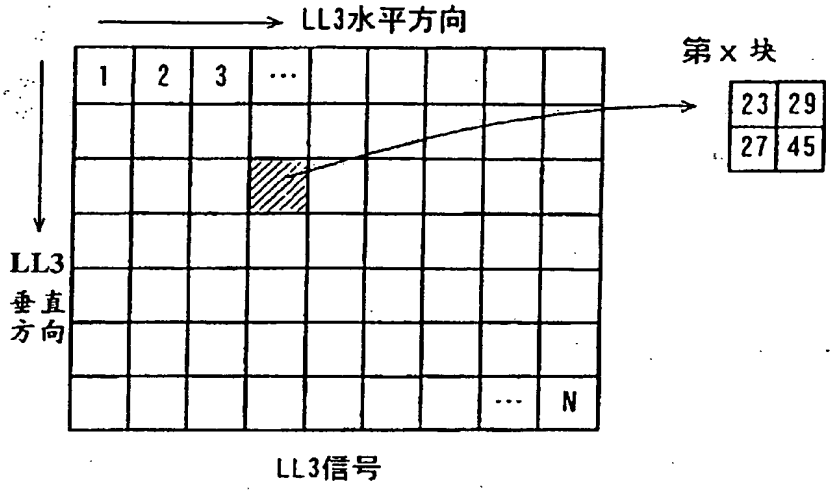


图 3

二级密钥	标志
r_1	0
r_2	1
r_3	0
⋮	⋮
⋮	⋮
r_{N-1}	1
r_N	1

图 4

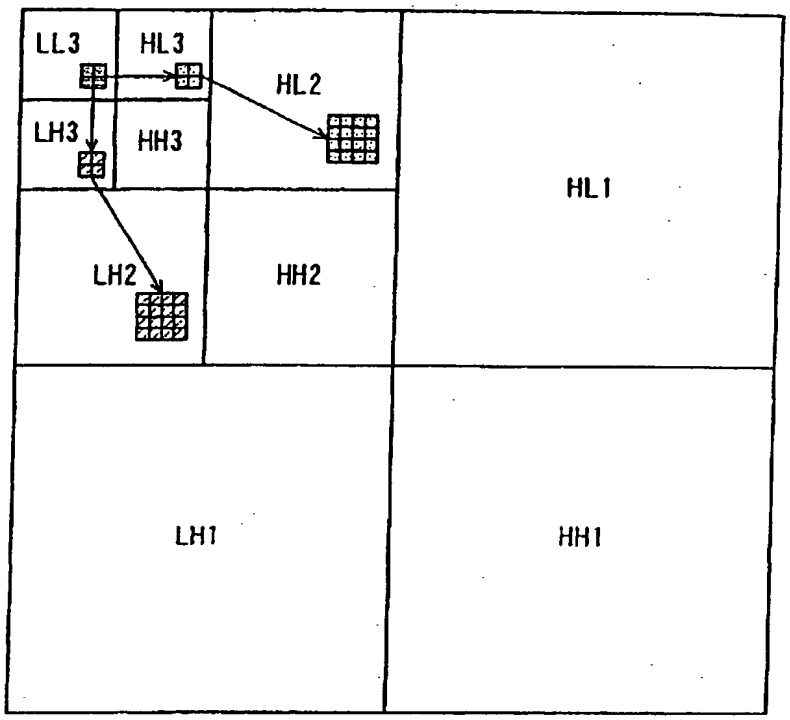


图 5

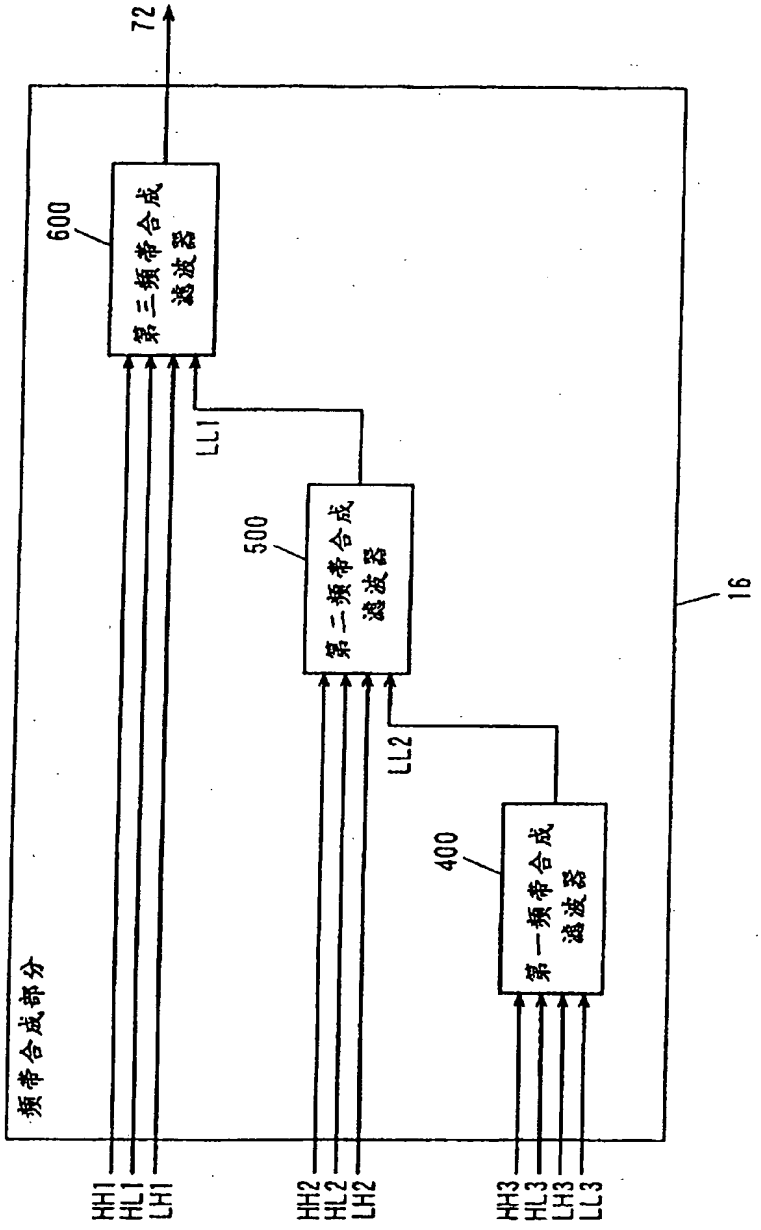

72
600
第三频带合成
滤波器
LL1
500
第二频带合成
滤波器
LL2
400
第一频带合成
滤波器
16
频带合成部分
HH1
HL1
LH1
HH2
HL2
LH2
HH3
HL3
LH3
LL3

图 6

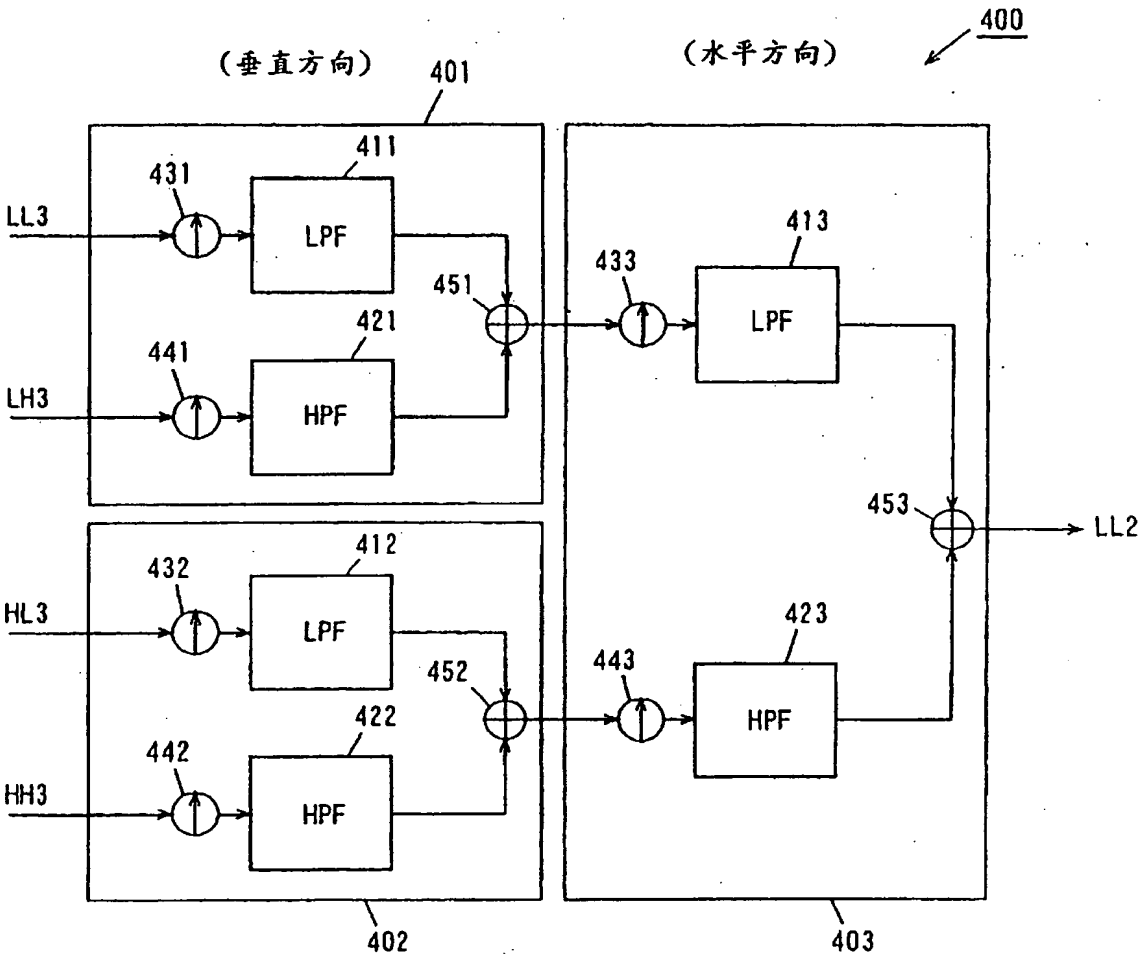

400
（垂直方向）
401
（水平方向）
411
431
LL3
LPF
451
421
441
LH3
HPF
413
433
LPF
453
LL2
412
432
HL3
LPF
452
423
443
HPF
422
442
HH3
HPF
402
403

图　7

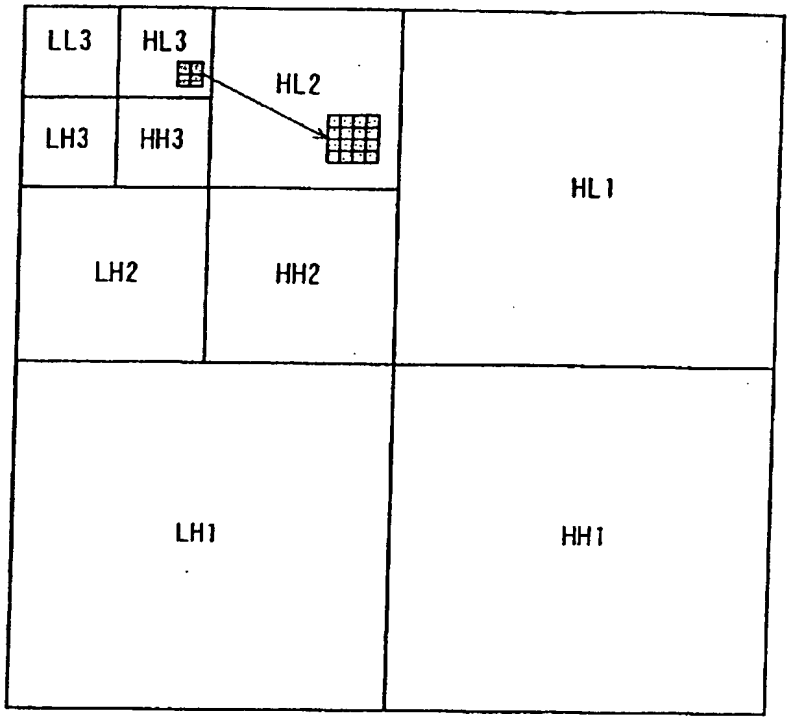


图 8

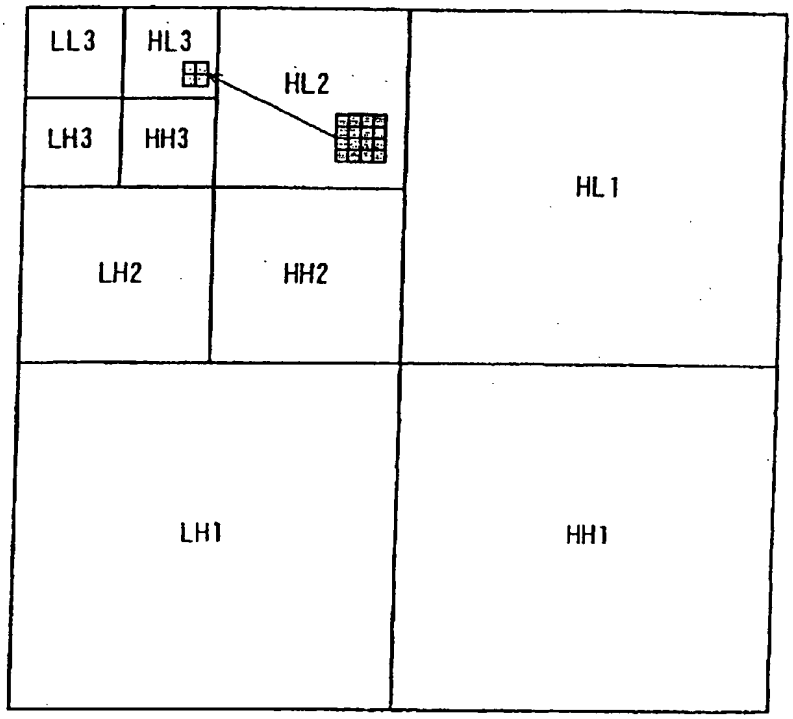


图 9

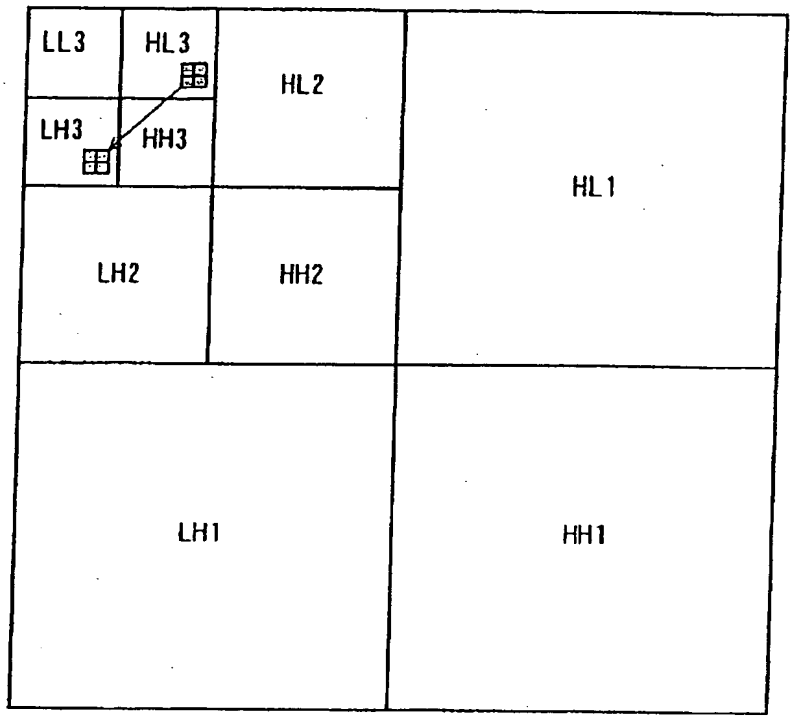


图 10

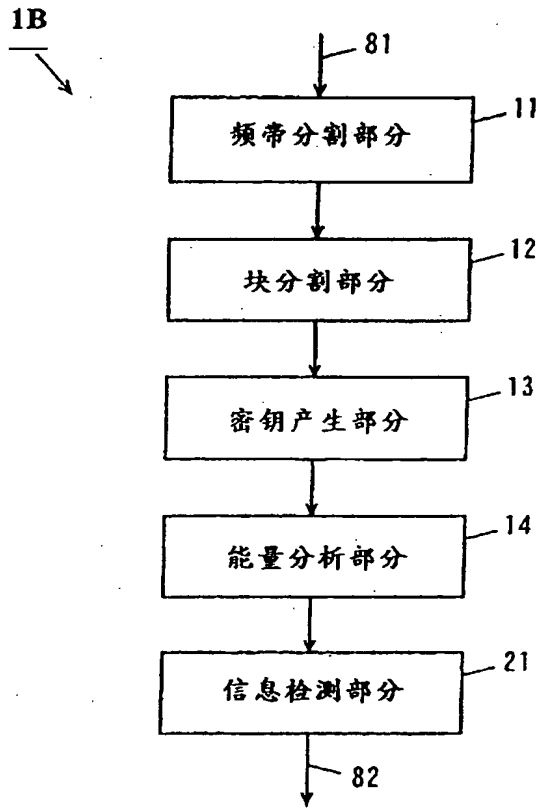


图 11

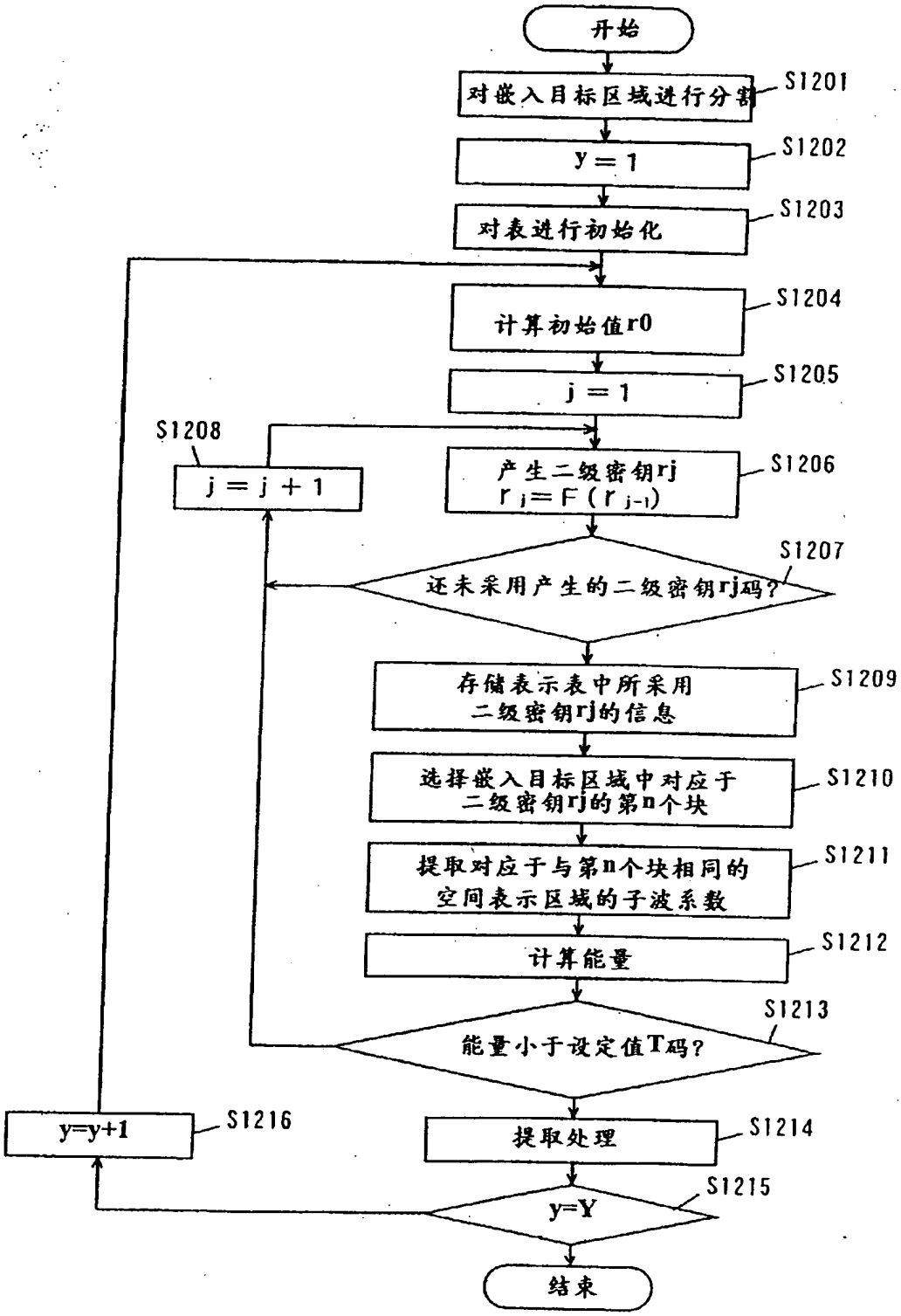

开始
对嵌入目标区域进行分割
S1201
y＝1
S1202
对表进行初始化
S1203
计算初始值r0
S1204
j＝1
S1205
产生二级密钥rj
$r_j = F(r_{j-1})$
S1206
还未采用产生的二级密钥rj码?
S1207
j＝j＋1
S1208
存储表示表中所采用
二级密钥rj的信息
S1209
选择嵌入目标区域中对应于
二级密钥rj的第n个块
S1210
提取对应于与第n个块相同的
空间表示区域的子波系数
S1211
计算能量
S1212
能量小于设定值T码?
S1213
提取处理
S1214
y=Y
S1215
y=y+1
S1216
结束

图　　12

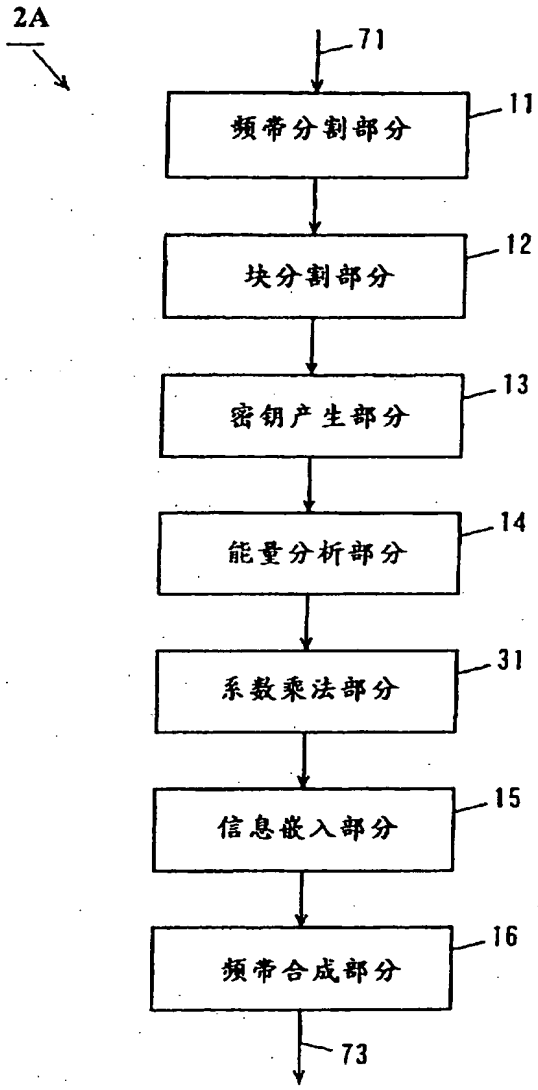

2A
71
频带分割部分
11
块分割部分
12
密钥产生部分
13
能量分析部分
14
系数乘法部分
31
信息嵌入部分
15
频带合成部分
16
73

图 13

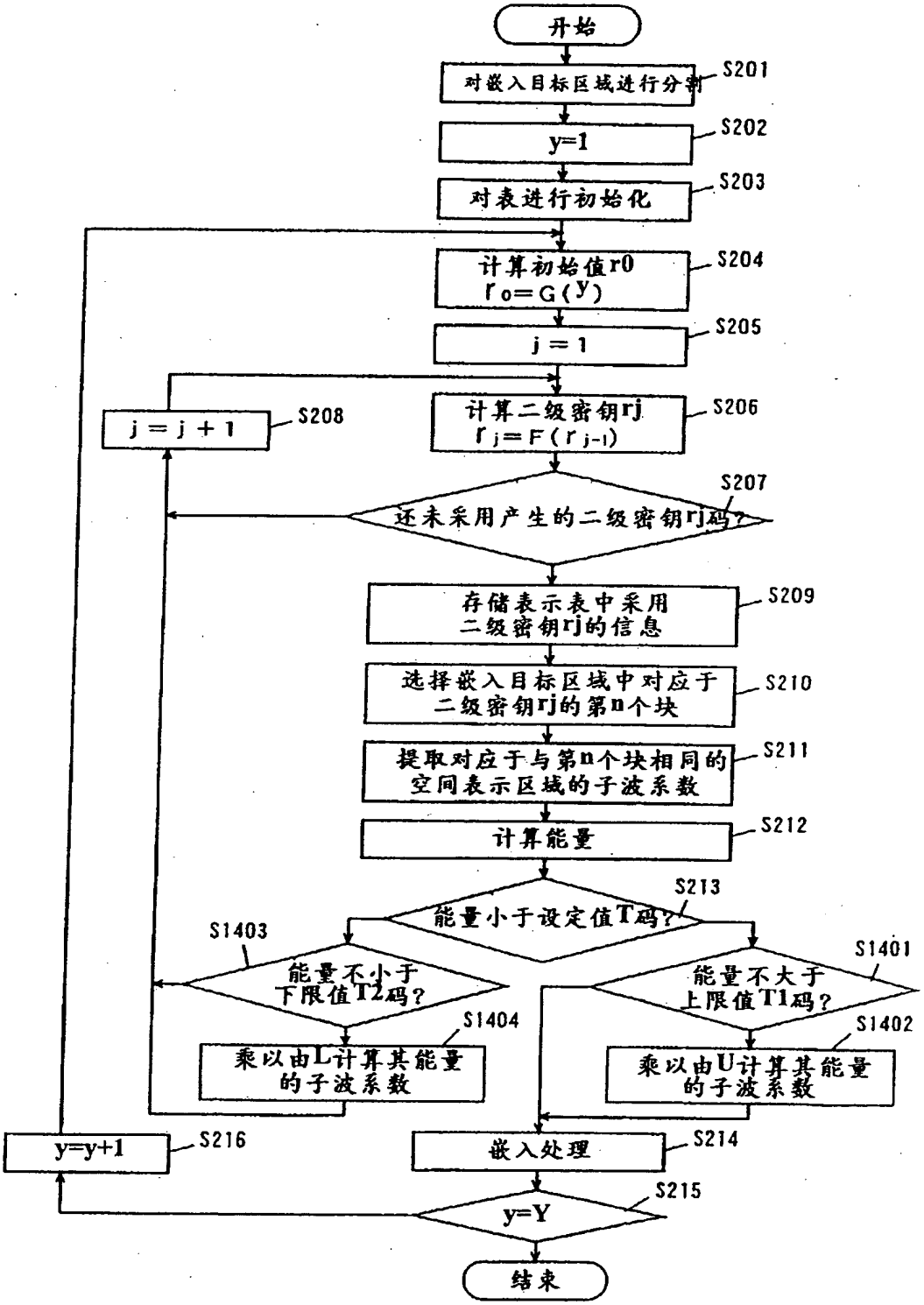

开始
对嵌入目标区域进行分割
S201
y=1
S202
对表进行初始化
S203
计算初始值r0
r o=G(y)
S204
j=1
S205
计算二级密钥rj
r j=F(r j-1)
S206
j=j+1
S208
还未采用产生的二级密钥rj码?
S207
存储表示表中采用
二级密钥rj的信息
S209
选择嵌入目标区域中对应于
二级密钥rj的第n个块
S210
提取对应于与第n个块相同的
空间表示区域的子波系数
S211
计算能量
S212
能量小于设定值T码?
S213
S1403
能量不小于
下限值T2码?
S1401
能量不大于
上限值T1码?
S1404
乘以由L计算其能量
的子波系数
S1402
乘以由U计算其能量
的子波系数
y=y+1
S216
嵌入处理
S214
y=Y
S215
结束

图 14

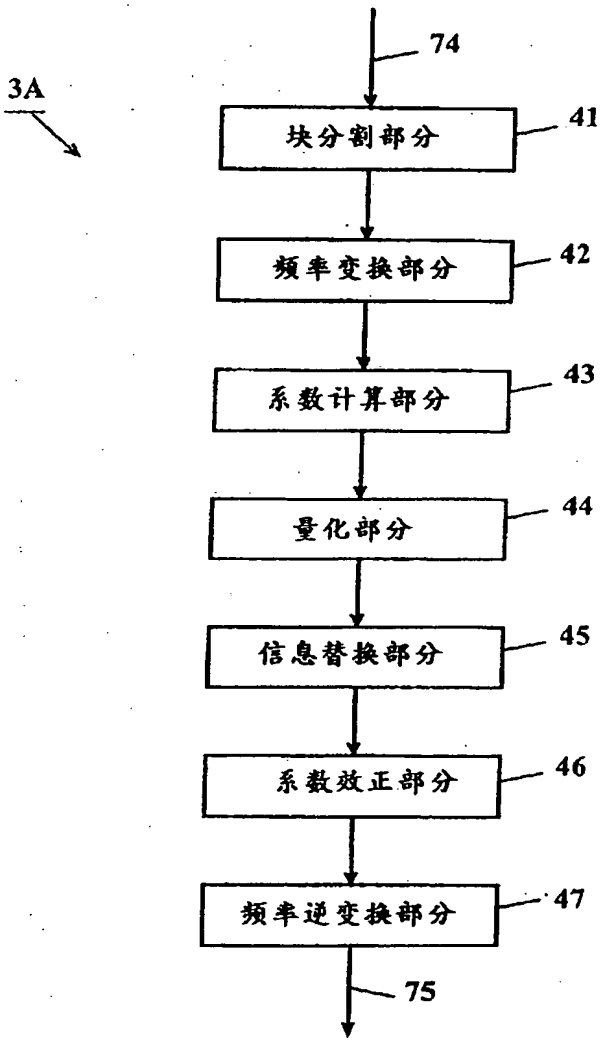

3A
74
块分割部分
41
频率变换部分
42
系数计算部分
43
量化部分
44
信息替换部分
45
系数效正部分
46
频率逆变换部分
47
75

图 15

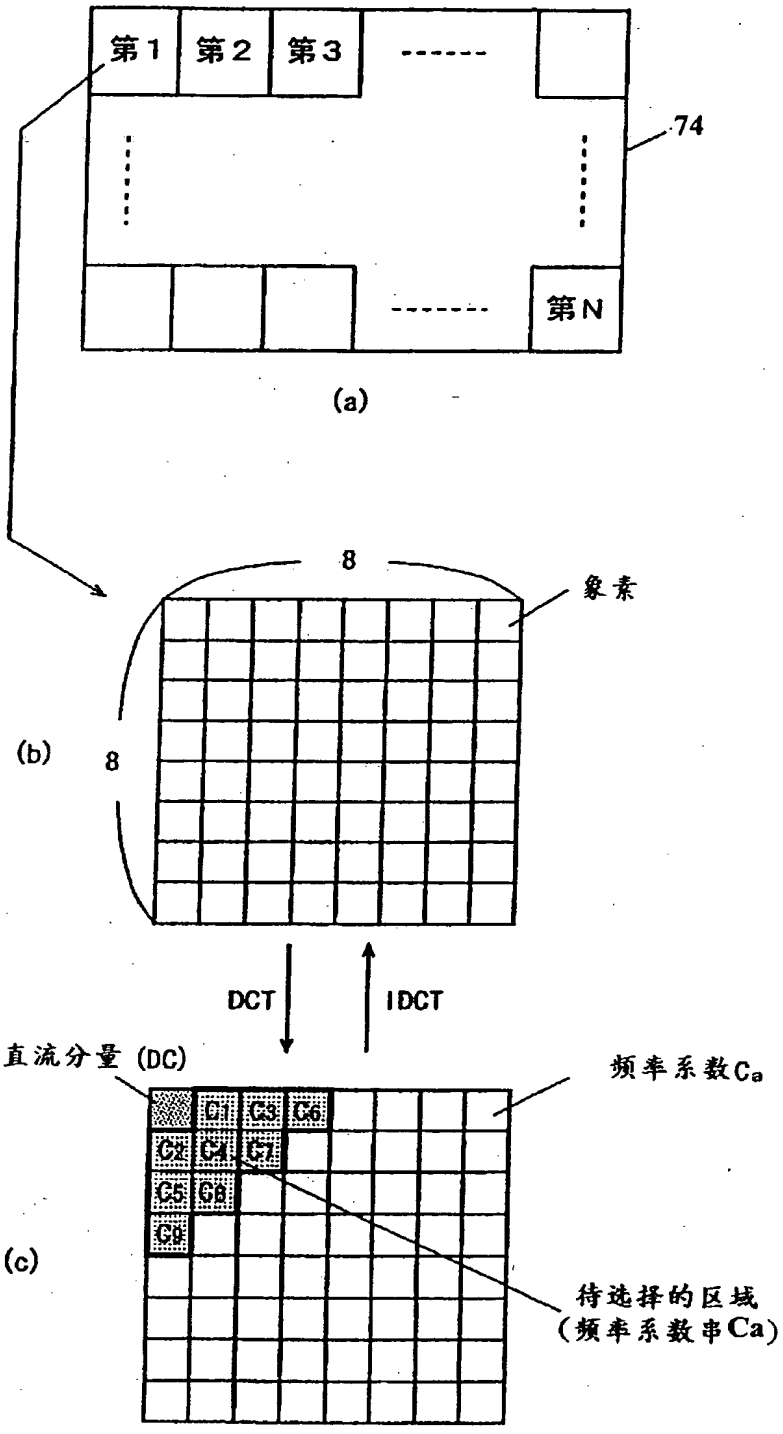

第1
第2
第3
第N
74
(a)
8
象素
(b)
8
DCT
IDCT
直流分量 (DC)
频率系数Ca
C1
C3
C6
C2
C4
C7
C5
C8
C9
(c)
待选择的区域
(频率系数串Ca)

图 16

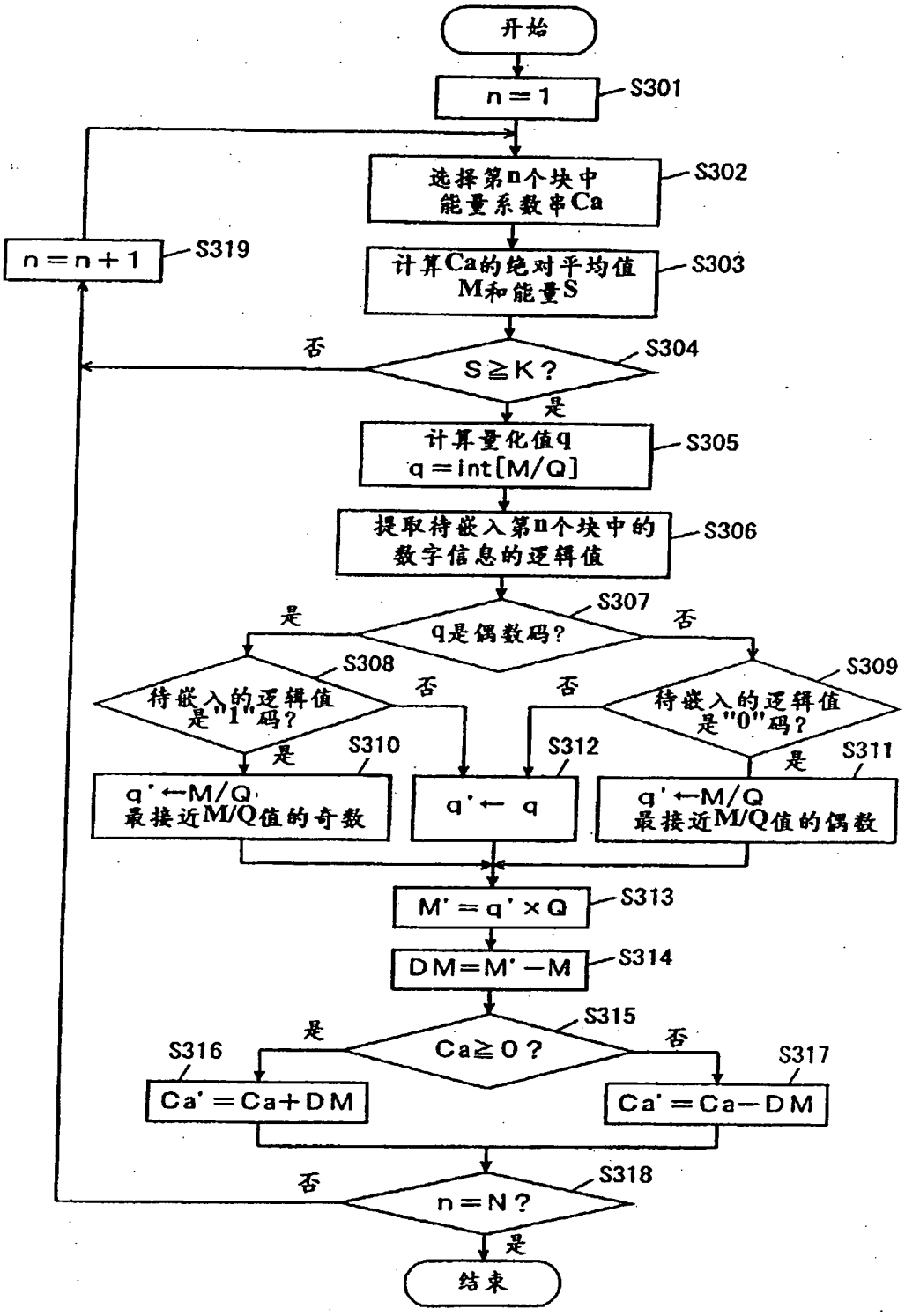

开始
n＝1
S301
选择第n个块中
能量系数串Ca
S302
计算Ca的绝对平均值
M和能量S
S303
S≧K？
S304
否
是
计算量化值q
q＝int[M/Q]
S305
提取待嵌入第n个块中的
数字信息的逻辑值
S306
q是偶数码？
S307
是
否
待嵌入的逻辑值
是"1"码？
S308
否
是
待嵌入的逻辑值
是"0"码？
S309
否
是
q'←M/Q
最接近M/Q值的奇数
S310
q'← q
S312
q'←M/Q
最接近M/Q值的偶数
S311
M'＝q'×Q
S313
DM＝M'－M
S314
Ca≧0？
S315
是
否
Ca'＝Ca＋DM
S316
Ca'＝Ca－DM
S317
n＝N？
S318
否
是
结束
n＝n＋1
S319

图　17

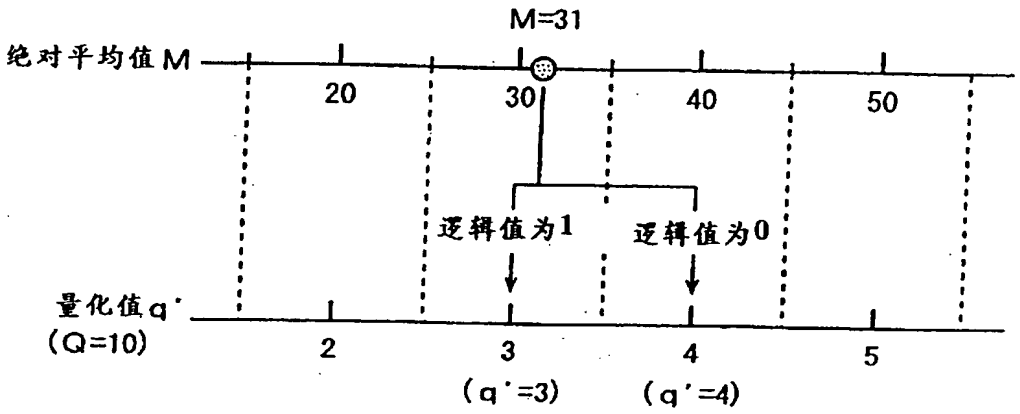

M=31
绝对平均值 M
20
30
40
50
逻辑值为1
逻辑值为0
量化值q'
(Q=10)
2
3
4
5
(q'=3)
(q'=4)

图 18

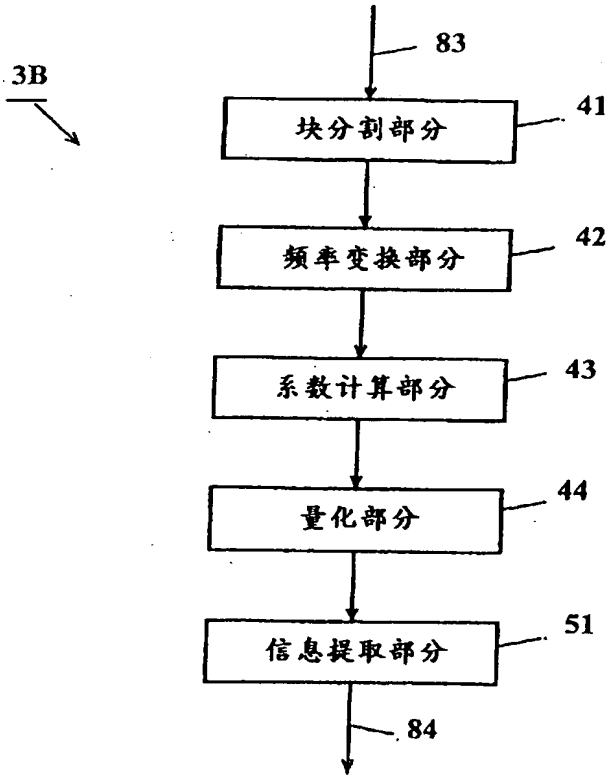

3B
83
块分割部分
41
频率变换部分
42
系数计算部分
43
量化部分
44
信息提取部分
51
84

图 19

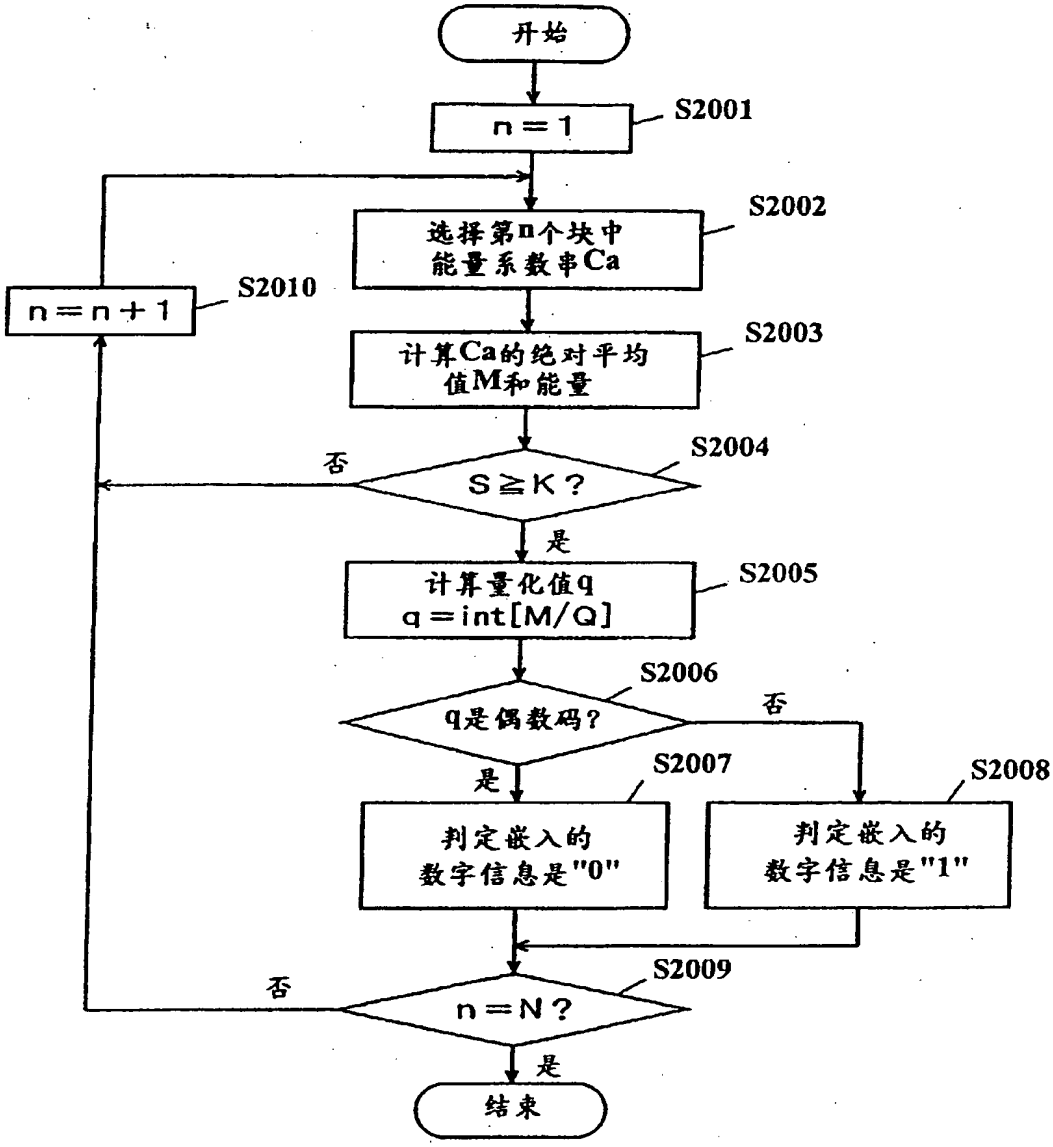

开始
n＝1
S2001
选择第n个块中
能量系数串Ca
S2002
计算Ca的绝对平均
值M和能量
S2003
S≧K？
S2004
否
是
计算量化值q
q＝int[M/Q]
S2005
q是偶数码？
S2006
否
是
判定嵌入的
数字信息是"0"
S2007
判定嵌入的
数字信息是"1"
S2008
n＝N？
S2009
否
是
结束
n＝n＋1
S2010

图　20

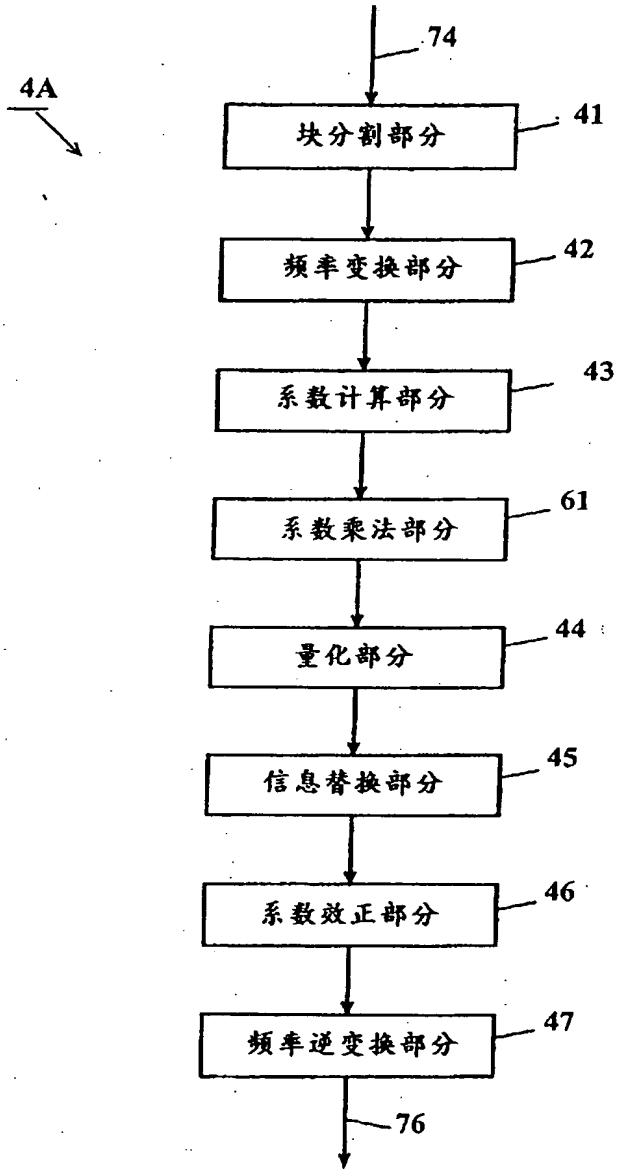

4A
74
块分割部分
41
频率变换部分
42
系数计算部分
43
系数乘法部分
61
量化部分
44
信息替换部分
45
系数效正部分
46
频率逆变换部分
47
76

图 21

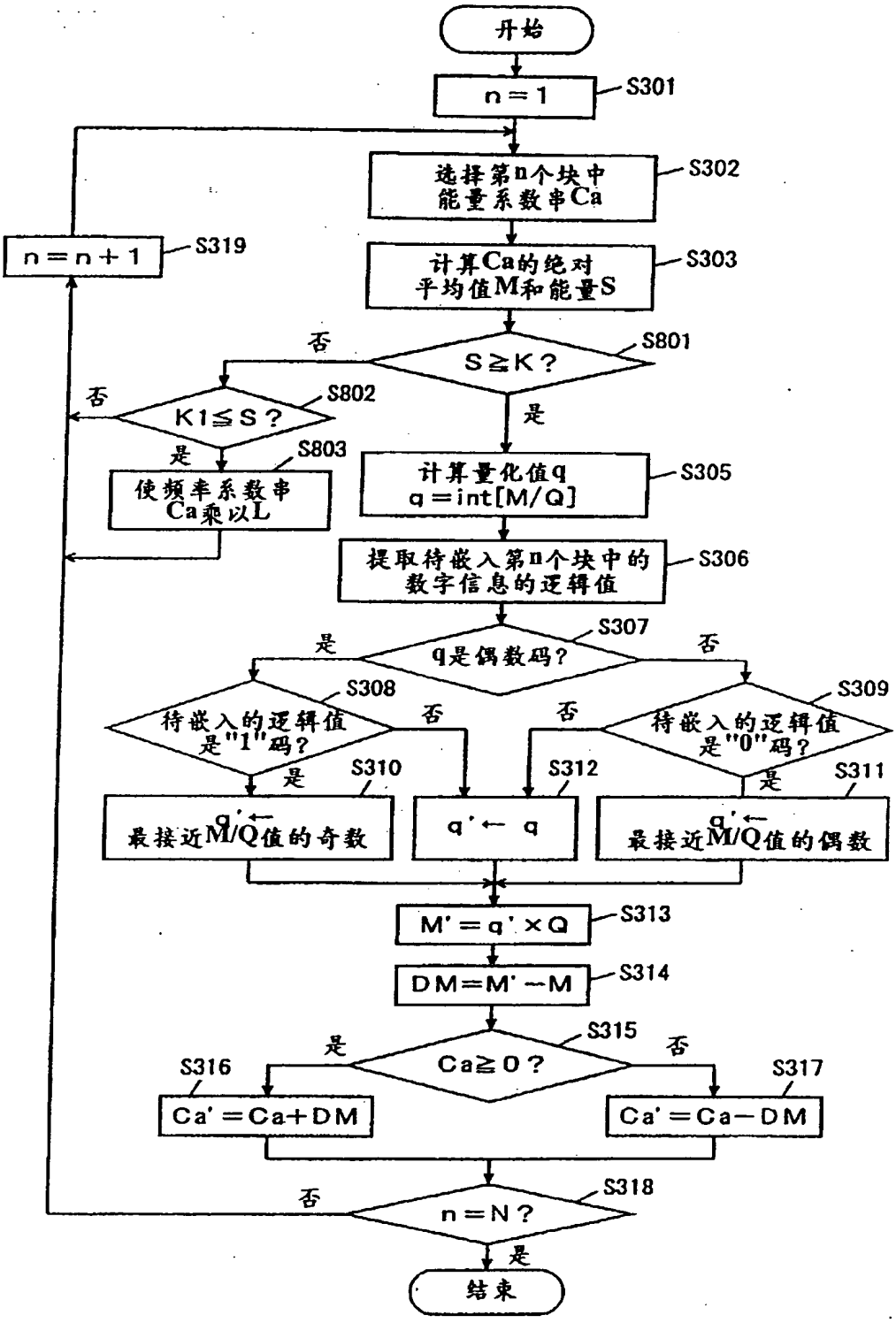

开始
n＝1
S301
选择第n个块中能量系数串Ca
S302
计算Ca的绝对平均值M和能量S
S303
S≧K？
S801
否
是
K1≦S？
S802
否
是
使频率系数串Ca乘以L
S803
计算量化值q
q＝int[M/Q]
S305
提取待嵌入第n个块中的数字信息的逻辑值
S306
q是偶数码？
S307
是
否
待嵌入的逻辑值是"1"码？
S308
否
是
待嵌入的逻辑值是"0"码？
S309
否
是
q'← 最接近M/Q值的奇数
S310
q'← q
S312
q'← 最接近M/Q值的偶数
S311
M'＝q'×Q
S313
DM＝M'－M
S314
Ca≧0？
S315
是
否
Ca'＝Ca＋DM
S316
Ca'＝Ca－DM
S317
n＝N？
S318
否
是
结束
n＝n＋1
S319

图 22

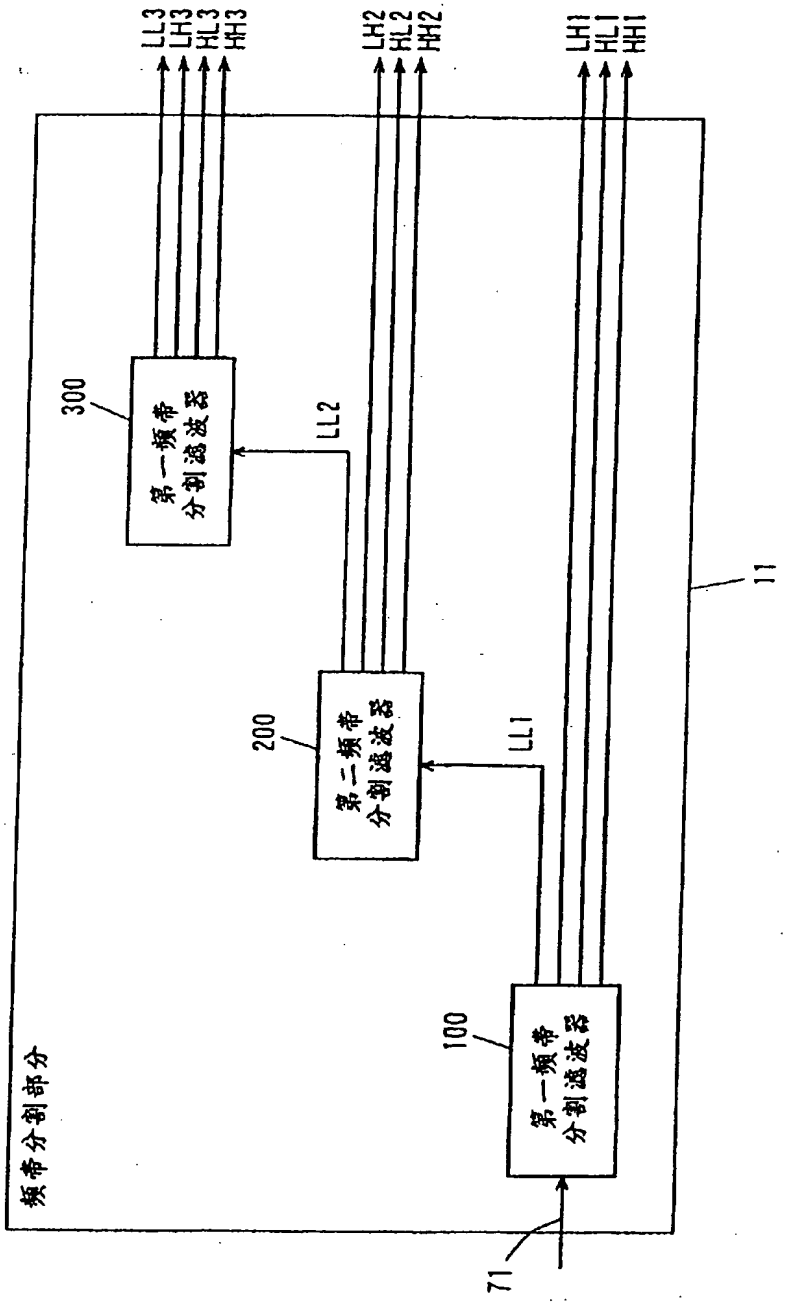

LL3
LH3
HL3
HH3
LH2
HL2
HH2
LH1
HL1
HH1
300
第一频带
分割滤波器
LL2
200
第二频带
分割滤波器
LL1
100
第一频带
分割滤波器
频带分割部分
11
71

图 23

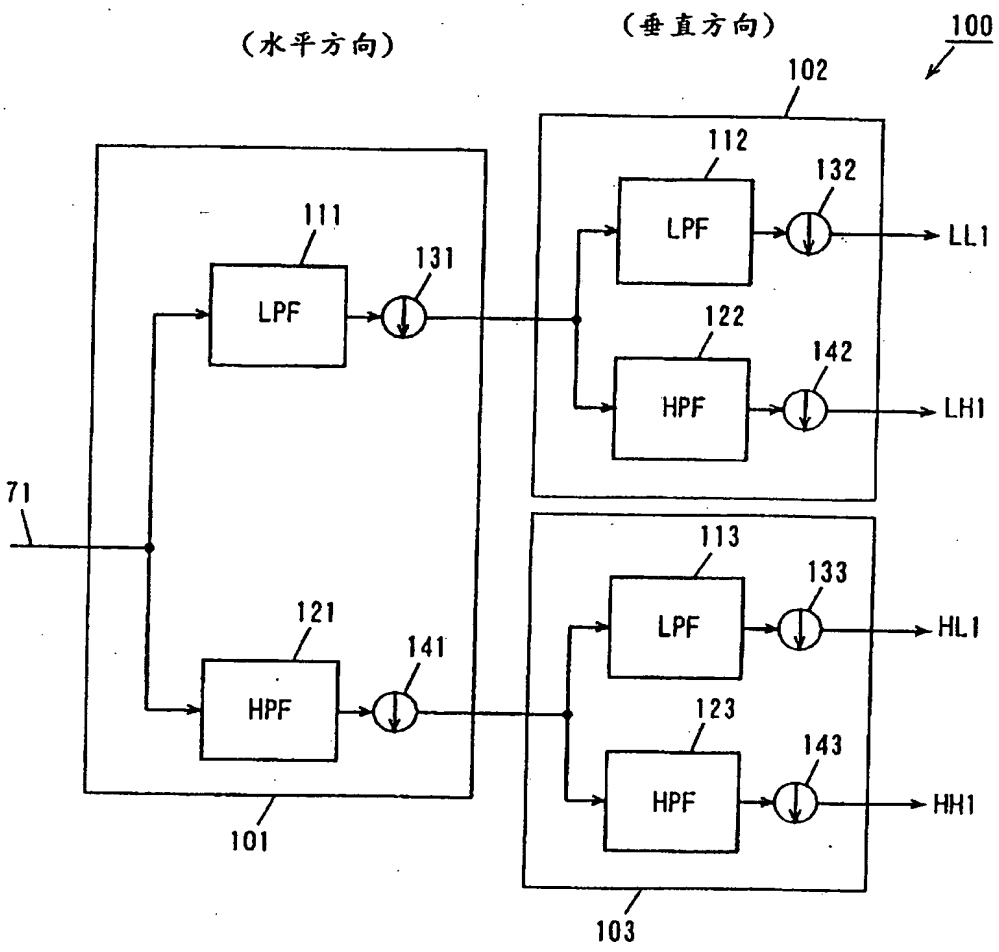

（水平方向）
（垂直方向）
100
102
112
132
LPF
LL1
111
131
LPF
122
142
HPF
LH1
71
113
133
LPF
HL1
121
141
HPF
123
143
HPF
HH1
101
103

图　24

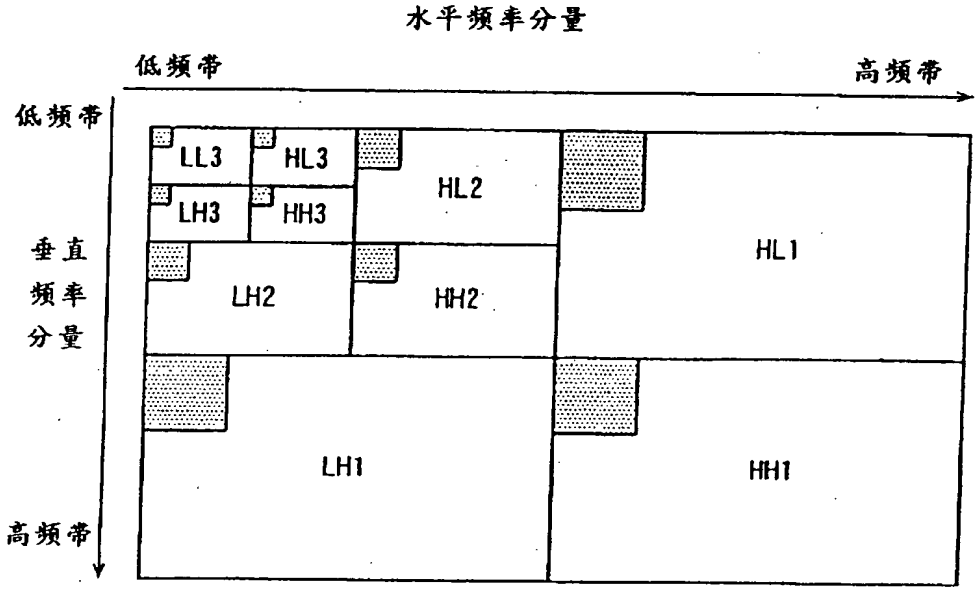

水平频率分量
低频带
高频带
低频带
垂直
频率
分量
高频带
LL3
HL3
HL2
LH3
HH3
HL1
LH2
HH2
LH1
HH1

图 25